3
artigo geral
VOL. 48 - N.1

Tecnologias Quânticas em Criptografia

Nuno A. Silva[1], Maurício Ferreira[1,2], Sara Mantey[1,2], Margarida Almeida[1,2], Gustavo Anjos[1], Nelson J. Muga[1], Armando N. Pinto[1,2]

[1]Instituto de Telecomunicações e Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

[2]Departamento de Eletrónica, Telecomunicações e Informática, Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

nasilva@ua.pt

Resumo

A segurança e a privacidade dos nossos dados digitais são atualmente garantidas assumindo que entidades sem acesso legítimo aos mesmos dispõem de capacidades computacionais limitadas. Contudo, recentes desenvolvimentos alcançados nas áreas da computação em rede e da computação quântica prometem colocar desafios inultrapassáveis aos protocolos criptográficos implementados nos atuais dispositivos. Em particular, os protocolos criptográficos de chave assimétrica são conhecidos pelas suas vulnerabilidades a ataques baseados em computação quântica. No entanto, uma nova classe de protocolos criptográficos baseados nos princípios da mecânica quântica oferecem uma abordagem inovadora, capaz de solucionar o problema de segurança e privacidade na proteção dos dados.

Introdução

A criptografia quântica, ou mais especificamente, o uso das propriedades quânticas para a codificação e descodificação de informação secreta nasceu com Stephen Wieser em 1983 [1]. Esse trabalho pioneiro deu origem a uma nova área de investigação e desenvolvimento, isto é a criptografia quântica. Atualmente, a codificação de informação através de criptografia clássica baseia-se na complexidade de certos problemas matemáticos, tal como a factorização de números inteiros, os quais um computador clássico pode demorar séculos a resolver [2], [3]. Os computadores quânticos têm a capacidade de resolver certos problemas matemáticos muito mais rapidamente que computadores clássicos. Um exemplo desses problemas é precisamente a factorização de números inteiros, colocando dessa forma em causa a segurança da criptografia clássica e, consequentemente, a confidencialidade de grande parte da informação que atualmente circula pela Internet [4]. Como termo de comparação, um processador quântico fotónico desenvolvido em 2022 resolveu uma tarefa especifica (amostragem de bosões) em 36 microssegundos, enquanto um computador clássico teria precisado de 9000 anos [5].

A criptografia quântica tem como objetivo principal o uso das propriedades da mecânica quântica para encriptar e transmitir dados num canal de comunicação de forma segura. Um dos exemplos mais conhecidos nesta área de investigação é a geração e distribuição de chaves simétricas em canais de comunicação públicos, usualmente denominada de distribuição quântica de chaves (QKD). De forma detalhada, entidades que pretendem comunicar de forma segura recorrem à QKD para criarem uma chave simétrica secreta que permita codificar e descodificar uma dada mensagem de forma segura. Ao contrário da criptografia clássica, a criptografia quântica é segura independentemente da capacidade computacional que um adversário possa ter [6]. Isto porque a segurança da QKD baseia-se nas propriedades de efeitos quânticos que se regem pelos princípios da mecânica quântica, tais como o princípio da incerteza e o princípio da não clonagem. Fazendo uso desses princípios, é sempre possível detetar a presença de um espião que tenta atacar o sistema durante a implementação do protocolo que permite gerar uma chave secreta entre duas entidades separadas no espaço.

Os protocolos de QKD dividem-se em duas categorias principais, dependendo do uso de variáveis discretas (DV-QKD) ou de variáveis contínuas (CV-QKD). DV-QKD corresponde ao método inicialmente proposto para a distribuição de chaves e baseia-se no uso das propriedades discretas de fotões únicos para gerar a chave secreta [7]. Mais recentemente, foi proposto o uso das propriedades contínuas dos estados coerentes para extrair uma chave secreta, denominada de CV-QKD [8], [9]. Para além destas duas categorias de sistemas de QKD, existe uma terceira categoria que é baseada nas propriedades do entrelaçamento quântico. Esta categoria de sistemas QKD foi proposta em 1991 por Artur Ekert [6]. Apesar de ser um aspeto frequentemente negligenciado, é fundamental garantir que as chaves geradas pelos sistemas de criptografia quântica possuem propriedades adequadas ao fim a que se destinam. Como descrito pelo princípio de Kerckhoffs [10], a imprevisibilidade da chave criptográfica é determinante para a segurança de um protocolo de QKD. Assim, a segurança destes sistemas criptográficos depende implicitamente da qualidade da fonte de entropia utilizada e, por conseguinte, do gerador de números aleatórios (RNG) escolhido para a implementação das diferentes fases dos protocolos [11]. Se do RNG resultarem sequências correlacionadas, ou o método de geração de aleatoriedade for passível de ser manipulado por um adversário, a segurança do protocolo não é garantida [12].

Até agora, os geradores pseudoaleatórios (PRNGs) têm sido a abordagem mais utilizada para a obtenção da aleatoriedade requeridas pelos protocolos. Infelizmente, estes geradores são deterministas e inerentemente periódicos, tornando-se previsíveis para um adversário com recursos computacionais suficientes

[13]. Na verdade, estes ataques criptoanalíticos a PRNGs são cada vez mais comuns devido à crescente capacidade computacional e a técnicas emergentes como Machine Learning (ML) que permitem identificar padrões nas sequências aleatórias [14]. Adicionalmente, PRNGs são particularmente vulneráveis à introdução de backdoors e a falhas catastróficas por erros de implementação, tendo sido já responsáveis por diversos ataques bem-sucedidos [15]. Assim, apesar de existirem implementações consideradas criptograficamente seguras, a sua fiabilidade a longo prazo não pode ser garantida.

Geradores quânticos de números aleatórios (QRNGs) exploram as propriedades das medições de fenómenos quânticos para colmatar as falhas de segurança dos seus homólogos clássicos. Ao contrário dos últimos [16], [17], a sua fonte de aleatoriedade não se baseia numa mera dificuldade em modelar um sistema determinístico complexo, fundamentando-se antes num processo inerentemente probabilístico [11]. Tal torna estes sistemas particularmente atrativos para aplicações criptográficas.

Geração quântica de números aleatórios

As primeiras propostas para QRNGs exploravam a aleatoriedade associada aos processos de decaimentos radioativos, o que, dada a sua natureza, dificultava em muito a sua implementação em termos práticos [18]. Em geral, os esquemas contemporâneos exploram as propriedades quânticas de sistemas óticos, que, para além de permitirem implementações muito mais práticas e seguras do ponto de vista da integridade do utilizador, permitem também alcançar taxas de geração muito mais elevadas. Uma outra vantagem destes sistemas óticos é o facto de utilizarem tecnologias eletro-ópticas largamente utilizadas em sistemas telecomunicações clássicos atualmente implementados [11]. Tal como na QKD, estas fontes de entropia subdividem-se entre as que medem propriedades discretas de fotões únicos [19], [20] e as que analisam variáveis contínuas [10]. Apesar de a primeira abordagem ser conceptualmente mais simples, a deteção macroscópica evita limitações associadas às técnicas de deteção de fotões únicos, como o dead time dos detetores, permitindo fornecer taxas de geração mais elevadas [11]. Desta forma, sistemas que exploram fenómenos tão diversos como a emissão espontânea amplificada [21], [22], o espalhamento estimulado de Raman [23], o ruído de fase de um laser [24], ou as flutuações de quadratura de um estado vácuo [25], [26], foram já implementados. Não obstante o desempenho obtido ser dependente de cada implementação e da fonte de entropia escolhida, foram já demonstradas taxas de geração de números aleatórios até 100 Gbps [27].

Apesar de intrinsecamente probabilísticas, outras fontes de ruído de origem clássica, como o ruído eletrónico, estão geralmente presentes nos geradores quânticos. Consequentemente, algoritmos de extração de aleatoriedade computacionalmente exigentes são normalmente necessários para obter uma implementação informação-teoricamente segura [28]. A maioria destes protocolos de geração assume um adversário passivo, incapaz de ativamente manipular o gerador, e fundamenta a sua segurança numa caracterização extensiva da implementação experimental [29]. Desta forma, estas implementações permanecem geralmente vulneráveis a formas de manipulação ativas como controlo da temperatura [30], [31]. Ainda assim, existem QRNGs que oferecem uma segurança independente dos diversos componentes que os compõem, garantindo a aleatoriedade e privacidade das chaves geradas através da verificação de desigualdades de Bell [32], [33]. Estes esquemas fornecem o maior nível de segurança possível, removendo a necessidade de confiar na própria implementação, mas sacrificam gravemente as taxas de geração alcançáveis. Como um compromisso entre estas duas abordagens, implementações híbridas que mantêm a confiança apenas em parte do gerador, tipicamente na fonte ótica [34], [35] ou no sistema de medição [36], [37], têm-se tornado cada vez mais populares. Adicionalmente, uma área de desenvolvimento importante tem sido a sua implementação em plataformas fotónicas integradas capazes de se aproximar dos custos e facilidade de utilização dos PRNGs tradicionais [38], [39]. Recentemente, integrámos um gerador de números aleatórios baseado nas flutuações de quadratura de um estado vácuo num servidor de rede, podendo este ser acedido remotamente.

Criptografia quântica com variáveis discretas

Os sistemas DV-QKD baseiam-se na utilização de propriedades discretas de fotões únicos, como a polarização, para codificar a chave secreta [40]. Neste caso, o transmissor, geralmente conhecido como Alice, prepara os fotões modulando a sua polarização de acordo com duas sequências de números aleatórios, uma das quais serve para definir a unidade de informação quântica (geralmente denominado qubit) a ser codificada e a segunda servirá para definir a base a ser usada para codificar o mesmo qubit. De seguia, a Alice envia os fotões para o recetor, geralmente conhecido por Bob. O Bob, por sua vez, mede a polarização dos fotões recebidos utilizando detetores de fotões únicos. As especificações que a Alice e o Bob usam para enviar/receber os fotões são definidos pelo protocolo QKD a ser aplicado.

O primeiro protocolo de QKD foi desenvolvido em 1984 por Charles Bennett e Giles Brassard, sendo conhecido como protocolo BB84 [7]. No total, existem seis estados de polarização que per-

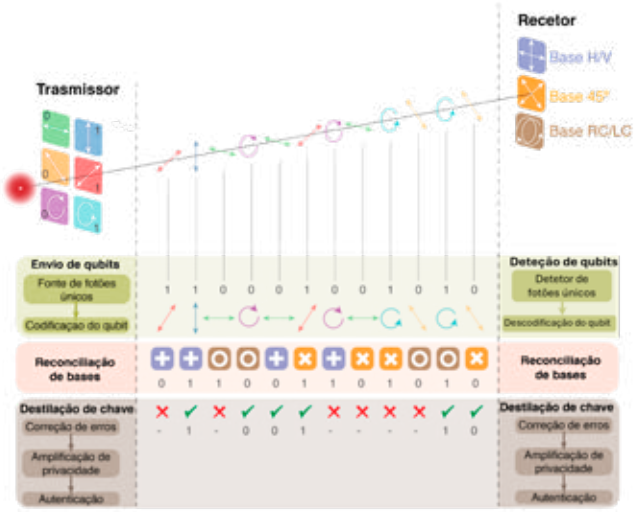

Figura 1 - Representação esquemática do princípio de funcionamento de um protocolo de QKD. No transmissor são representados os seis estados de polarização que podem ser usados para codificar os qubits, enquanto no recetor estão representadas as três bases correspondentes. Apos a codificação da chave usando a polarização dos fotões únicos, estes são enviados para o recetor onde é feita a respetiva descodificação. Após esta fase dá se a reconciliação de bases e a destilação da chave que dará como produto final uma chave secreta e simétrica no transmissor e recetor.

tencem a três bases mutuamente não ortogonais: a base retilínea que inclui os estados de polarização horizontal e vertical, a base diagonal, com os estados diagonal e anti-diagonal, e a base circular que engloba os estados circular direito e circular esquerdo, tal como mostra a Fig. 1. Na implementação do BB84, são usados quatro destes seis estados, por exemplo, os estados das bases retilínea e circular. Assim, Alice gera duas sequências de números aleatórios utilizando um QRNG para codificar os qubits. Uma destas sequências decide a base a usar e a outra o estado dessa mesma base. Por exemplo, o valor '0' da primeira sequência corresponderia à base retilínea e o valor '1' à base circular. Da mesma forma, o valor '0' da segunda sequência corresponderia ao estado horizontal ou circular direito, enquanto o valor '1' corresponderia ao estado vertical ou circular esquerdo. No recetor, Bob gera apenas uma sequência de números aleatórios que definem em que base ele vai medir a polarização dos fotões que recebe. Após a medição da polarização, dada de forma discreta através da observação de qual dos dois detetores de fotões únicos deu clique, ele regista qual a polarização medida e em que base foi realizada a medição. Dado que Bob escolhe aleatoriamente a base em que vai medir, ele apenas vai acertar nas bases usadas pela Alice em 50% dos fotões recebidos. Nos casos em que as bases da Alice e do Bob não coincidem, a medição da polarização tem 50% de probabilidade de estar correta e 50% de estar errada. De seguida, Alice e Bob tornam público que bases utilizaram para a codificação/medição. Nos casos em que não escolheram a mesma base o qubit é descartado, enquanto os qubits em que as bases coincidem correspondem à chave secreta que vão usar para codificar e descodificar a mensagem secreta que pretendem partilhar. O processo de obtenção da chave a partir dos bits enviados é conhecido por destilação da chave.

Devido a perturbações no canal através do qual são enviados os fotões, pode haver erros na chave partilhada entre Alice e Bob que precisam de ser corrigidos. Para estimar a percentagem de erros existentes na chave, parte desta é partilhada através de um canal público. Ao parâmetro que define a taxa quântica de erros existentes denomina-se de quantum bit error rate (QBER). Durante a correção de erros perde-se alguma segurança da chave, dado que é partilhada informação no canal público obtida a partir da chave. Assim, é necessário proceder à amplificação da privacidade e de seguida à autenticação [41].

A deteção de um espião, geralmente chamado Eve, é feita através da medição do QBER mencionado anteriormente. Como entidade externa, a Eve não sabe quais foram as bases escolhidas pela Alice na fase de codificação e, numa tentativa de conseguir obter informação sobre os fotões enviados para o Bob, vai fazer as suas medidas escolhendo as suas bases de medição de forma aleatória. Este aspeto faz com que a Eve acerte nas bases em apenas 50% das suas medições. De notar que, de acordo com a mecânica quântica (particularmente o teorema da não-clonagem) um estado quântico desconhecido não pode ser clonado. Do ponto de vista do espião no canal quântico, isto significa que sempre que as bases da Alice e da Eve não coincidam o estado enviado pela Alice não poderá ser clonado pela Eve. Nos restantes 50% em que não acertou na base, o resultado da medição da polarização vai ser aleatório. Desta forma, se a Eve decidir reenviar para o Bob os fotões com a polarização que mediu, numa tentativa de não ser detetada, a Alice e o Bob, ao comparem as suas chaves vão aperceber-se que tem cerca de 25% de erros, conseguindo detetar a presença de um espião [41]. Para provar a segurança do protocolo e para estimar a quantidade de informação que a Eve consegue alcançar, consoante a probabilidade de ser detetada, existem as provas de segurança. Estas provas geralmente usam argumentos da teoria de informação e dão uma estimativa de quanta informação terá de ser sacrificada para garantir que a Eve não obteve informação nenhuma [42] [43].

Distribuição de chaves quânticas com variáveis contínuas

Os sistemas CV-QKD fazem uso das propriedades dos estados coerentes para obter uma chave secreta, partilhada pela Alice e pelo Bob. Os estados coerentes são facilmente obtidos recorrendo a lasers comerciais [8], [9]. No geral, a CV-QKD faz uso de dispositivos comuns, bastante estudados e utilizados nas telecomunicações clássicas, tornando a implementação prática de sistemas CV-QKD não só mais barata, como mais simples do que a implementação dos sistemas DV-QKD [44], [45], [46]. Num protocolo de CV-QKD tradicional, a Alice modela as quadraturas de estados coerentes tendo por base modelação Gaussiana ou modelação discreta [9], [47], [48]. O sinal laser que a Alice usa é bastante atenuado antes de ser transmitido. O Bob recorre a deteção coerente clássica, com o apoio de um sinal laser de alta intensidade, para medir as quadraturas do sinal enviado pela Alice. Dependendo do tipo de deteção usada, deteção homodína ou heterodína, o Bob consegue medir apenas uma ou as duas quadraturas do sinal, respetivamente. O uso de deteção heterodína permite usar o canal de forma mais eficiente e não requer a reconciliação de base, tal como exigido nos sistemas DV-QKD [49]. A segurança de um sistema CV-QKD considera, usualmente, o uso de modelação Gaussiana ideal para modelar os estados coerentes [50], [51]. No entanto, apesar de, teoricamente, este formato ter um desempenho ótimo [52], a sua implementação prática revela-se desafiante, acabando por ser muito difícil obter uma modelação Gaussiana ideal [50], [53]. Como tal, tem vindo a aumentar a aplicação de modelação discreta para modelar os estados coerentes [48]. Os formatos de modelação discreta são equivalentes aos usados nas comunicações clássicas, no entanto, ainda não foi obtida uma prova de segurança incondicional tendo em conta os ataques mais poderosos que um espião pode efetuar. Mesmo assim, já foi possível concluir que, recorrendo ao uso de modelação discreta de ordem elevada, é possível aproximar o desempenho da modelação Gaussiana [50], simplificando a implementação prática.

Para determinar a segurança da informação que a Alice e o Bob têm após a transmissão, a Alice e o Bob recorrem à estimação de parâmetros [54]. Durante este processo, é possível estimar os parâmetros do canal, especialmente o ruído associado a um potencial espião. Para tal, é necessário partilhar parte da informação que cada um tem, conseguindo, com isso, estimar a tamanho máximo da chave que podem extrair. A informação partilhada é descartada, não sendo utilizada nas fases posteriores do protocolo.

É de notar que a informação adquirida pelo Bob é ruidosa [55], e que, tanto a informação gerada pela Alice, como a adquirida pelo Bob, são compostas por valores reais, e não por valores binários. O passo denominado por reconciliação de informação é responsável por extrair uma chave binária através da informação

transmitida no canal quântico, garantindo que o transmissor e o recetor adquirem uma sequência binária igual [56], [57]. A reconciliação das chaves é o passo mais exigente computacionalmente nos sistemas CV-QKD e o que mais dificulta a sua implementação em tempo real.

Após a reconciliação de informação, a sequência binária partilhada entre a Alice e o Bob é apenas parcialmente secreta [58], [59], visto que um adversário pode ter informação de parte desta sequência. Recorrendo à informação obtida durante a estimação de parâmetros, a Alice e o Bob aplicam o passo de amplificação de privacidade, de forma a extrair uma chave binária idêntica, completamente secreta [58], [59].

Atuais desafios da Criptografia Quântica

Novos desenvolvimentos em QRNGs têm-se focado principalmente em aumentar as taxas de geração que podem ser alcançadas. Neste âmbito, uma preocupação fundamental é a redução da penalização introduzida pela complexidade computacional dos algoritmos de extração de aleatoriedade [60]. Adicionalmente, técnicas para maximizar a entropia disponível têm sido propostas como a implementação de fontes de aleatoriedade paralelas [61], [62] ou a otimização da amostragem do ruído [63]. Além disso, recentemente, novos protocolos semi-independentes dos dispositivos baseados em limites de energia [64], [65] ou sobreposição [66] dos estados medidos têm ganho atenção. Estes permitem relaxar a confiança necessária no sistema de medição, mantendo as taxas de geração tipicamente associadas a esquemas CV independentes da fonte ótica.

Atualmente, o desenvolvimento dos sistemas CV-QKD a nível experimental centra-se no estudo de soluções que permitam aumentar a distância entre a Alice e o Bob para a qual é possível extrair chaves criptográficas secretas. Por outro lado, o aumento da taxa de chaves secretas é ainda um tópico de estudo pela comunidade científica. Nesse sentido, está a ser analisado a aplicação de multiplexagem por divisão de frequência e multiplexagem de polarização para transmitir a informação entre a Alice e o Bob [67], [68]. Adicionalmente, tendo vindo a ganhar o interesse do estudo de sistemas CV-QKD coexistentes com sistemas de comunicações clássicas, o estudo de sistemas CV-QKD com propagação do sinal através do espaço livre, e ainda o estudo de sistemas CV-QKD baseados em estados entrelaçados [69]. No futuro, espera-se que os sistemas de CV-QKD sejam cada vez mais compactos, sendo para tal integrados em chips fotónicos [69].

Agradecimentos

Este trabalho é financiado pela FCT/MEC através de fundos nacionais no âmbito do projeto PTDC/EEI-TEL/8017/2020. Este trabalho foi ainda suportado pelo financiamento FCT/MEC através das bolsas 2022.09584.BD, 2021.06085.BD e UI/BD/153377/2022, associadas respetivamente aos autores M. Ferreira, S. Mantey e M. Almeida.

Referências

[1] S. Wiesner, "Conjugate coding," ACM Sigact News, vol. 15, no. 1, pp. 78–88, 1983.
[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM review, vol. 41, no. 2, pp. 303–332, 1999.
[3] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," IEEE Communications Magazine, vol. 55, no. 2, pp. 116–120, 2017.
[4] A. Sharma and A. Kumar, "A survey on quantum key distribution," in 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019, pp. 1–4.
[5] L. S. Madsen et al., "Quantum computational advantage with a programmable photonic processor," Nature, vol. 606, no. 7912, pp. 75–81, 2022.
[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev Mod Phys, vol. 74, no. 1, p. 145, 2002.
[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in International Conference on Computer Systems and Signal Processing (ICCSSP), 1984, pp. 175–179.
[8] C. Weedbrook et al., "Gaussian quantum information," Rev Mod Phys, vol. 84, no. 2, pp. 621–669, May 2012, doi: 10.1103/RevModPhys.84.621.
[9] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Phys Rev Lett, vol. 88, no. 5, p. 057902, Jan. 2002, doi: 10.1103/PhysRevLett.88.057902.
[10] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys., vol. 89, no. 1, p. 15004, Feb. 2017, doi: 10.1103/RevModPhys.89.015004.
[11] V. Mannalatha, S. Mishra, and A. Pathak, "A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness," Quantum Inf Process, vol. 22, no. 12, p. 439, 2023, doi: 10.1007/s11128-023-04175-y.
[12] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, "Weak randomness seriously limits the security of quantum key distribution," Phys. Rev. A, vol. 86, no. 6, p. 62308, Dec. 2012, doi: 10.1103/PhysRevA.86.062308.
[13] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic attacks on pseudorandom number generators," in Fast Software Encryption, S. Vaudenay, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 168–188.
[14] N. D. Truong, J. Y. Haw, S. M. Assad, P. K. Lam, and O. Kavehei, "Machine Learning Cryptanalysis of a Quantum Random Number Generator," IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 403–414, 2019, doi: 10.1109/TIFS.2018.2850770.
[15] G. Markowsky, "The Sad History of Random Bits," Journal of Cyber Security and Mobility, vol. 3, no. 1, pp. 1–24, 2014, doi: https://doi.org/10.13052/jcsm2245-1439.311.
[16] G. and V. P. Marangon Davide G. and Vallone, "Random bits, true and unbiased, from atmospheric turbulence," Sci Rep, vol. 4, no. 1, p. 5490, Jun. 2014, doi: 10.1038/srep05490.
[17] J.-C. Hsueh and V. H.-C. Chen, "An ultra-low voltage chaos-based true random number generator for IoT applications," Microelectronics J, vol. 87, pp. 55–64, 2019, doi: https://doi.org/10.1016/j.mejo.2019.03.013.
[18] A. Alkassar, T. Nicolay, and M. Rohe, "Obtaining True-Random Binary Numbers from a Weak Radioactive Source," in Computational Science and Its Applications -- ICCSA 2005, O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 634–646.
[19] Y. Zhang et al., "A simple low-latency real-time certifiable quantum random number generator," Nat Commun, vol. 12, no. 1, pp. 1–8, 2021, doi: 10.1038/s41467-021-21069-8.
[20] L. Nguyen, P. Rehain, Y. M. Sua, and Y.-P. Huang, "Programmable quantum random number generator without postprocessing," Opt Lett, 2018, doi: 10.1364/ol.43.000631.
[21] Y. Guo et al., "40 Gb/s quantum random number generation based on optically sampled amplified spontaneous emission," APL Photonics, vol. 6, no. 6, p. 066105, Jun. 2021, doi: 10.1063/5.0040250.
[22] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, "Quantum Random Number Generation for 1.25-GHz Quantum Key Distribution Systems," Journal of Lightwave Technology, vol. 33, no. 13, pp. 2855–2859, 2015, doi: 10.1109/JLT.2015.2416914.
[23] P. J. Bustard et al., "Quantum random bit generation using energy fluctuations in stimulated Raman scattering," Opt Express, 2013, doi: 10.1364/oe.21.029350.
[24] M. Huang, Z. Chen, Y. Zhang, and H. Guo, "A Phase Fluctuation Based Practical Quantum Random Number Generator Scheme with Delay-Free Structure," Applied Sciences, vol. 10, no. 7, 2020, doi: 10.3390/app10072431.
[25] T. Gehring et al., "Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information," Nat Commun, vol. 12, Feb. 2021, doi: 10.1038/s41467-020-20813-w.
[26] M. J. Ferreira, N. A. Silva, A. N. Pinto, N. J. Muga, Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations, Applied Sciences, Vol. 11, No. 16, pp. 7413-1 - 7413-16, August, 2021.
[27] C. Bruynsteen, T. Gehring, C. Lupo, J. Bauwelinck, and X. Yin, "100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations," PRX Quantum, vol. 4, no. 1, p. 10330, Mar. 2023, doi: 10.1103/PRXQuantum.4.010330.
[28] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A, vol. 87, no. 6, p. 62327, Jun. 2013, doi: 10.1103/PhysRevA.87.062327.
[29] J. Thewes, C. Lüders, and M. Aßmann, "Eavesdropping attack on a trusted continuous-variable quantum random-number generator," Phys Rev A (Coll Park), 2019, doi: 10.1103/PhysRevA.100.052318.
[30] Y. and W. W. and M. X. and W. H. and D. Q. and M. Z. Li Yuanhao and Fei, "Analysis of the effects of temperature increase on quantum random number generator," The European Physical Journal D, vol. 75, no. 2, p. 69, Feb. 2021, doi: 10.1140/epjd/s10053-021-00087-7.
[31] P. R. Smith, D. G. Marangon, M. Lucamarini, Z. L. Yuan, and A. J. Shields, "Out-of-Band Electromagnetic Injection Attack on a Quantum Random Number Generator," Phys Rev Appl, 2021, doi: 10.1103/PhysRevApplied.15.044044.
[32] Y. Zhang et al., "Experimental Low-Latency Device-Independent Quantum Randomness," Phys Rev Lett, 2020, doi: 10.1103/PhysRevLett.124.010505.
[33] L. K. Shalm et al., "Device-independent randomness expansion with entangled photons," Nat Phys, vol. 17, no. 4, pp. 452–456, 2021, doi: 10.1038/s41567-020-01153-4.
[34] T. Wu, C.-H. Zhang, X.-Y. Zhou, J. Li, and Q. Wang, "Measurement-Device-Independent Quantum Random-Number Generator With Source Flaws," IEEE Photonics J, vol. 15, no. 6, pp. 1–5, 2023, doi: 10.1109/JPHOT.2023.3331547.
[35] A. Tavakoli, "Semi-Device-Independent Framework Based on Restricted Distrust in Prepare-and-Measure Experiments," Phys Rev Lett, vol. 126, no. 21, p. 210503, May 2021, doi: 10.1103/PhysRevLett.126.210503.
[36] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," Nat Commun, vol. 9, no. 1, pp. 1–7, 2018, doi: 10.1038/s41467-018-07585-0.
[37] B. Xu et al., "High speed continuous variable source-independent quantum random number generation," Quantum Sci Technol, vol. 4, no. 2, p. 025013, 2019, doi:

10.1088/2058-9565/ab0fd9.
[38] N. Leone et al., "An optical chip for self-testing quantum random number generation," APL Photonics, vol. 5, no. 10, p. 101301, Oct. 2020, doi: 10.1063/5.0022526.
[39] B. Bai et al., "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," Appl Phys Lett, vol. 118, no. 26, p. 264001, 2021, doi: 10.1063/5.0056027.
[40] S. T. Mantey, N. A. Silva, A. N. Pinto, N. J. Muga, Design and implementation of a polarization-encoding system for quantum key distribution, Journal of Optics (United Kingdom), Vol. 26, No. 6, pp. 075704 - 075704, June, 2024.
[41] V. Martin, J. Martinez-Mateo, and M. Peev, "Introduction to quantum key distribution," Wiley Encyclopedia of Electrical and Electronics Engineering, pp. 1–17, 2017.
[42] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication," Phys Rev Lett, vol. 95, no. 8, p. 80501, 2005.
[43] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum--key-distribution protocols," Phys Rev A (Coll Park), vol. 72, no. 1, p. 12332, 2005.
[44] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement--device-independent quantum key distribution," Phys Rev A (Coll Park), vol. 89, no. 5, p. 052301, May 2014, doi: 10.1103/PhysRevA.89.052301.
[45] R. Namiki, A. Kitagawa, and T. Hirano, "Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers," Phys Rev A (Coll Park), vol. 98, no. 4, p. 042319, Oct. 2018, doi: 10.1103/PhysRevA.98.042319.
[46] P. Huang, J. Fang, and G. Zeng, "State-discrimination attack on discretely modulated continuous-variable quantum key distribution," Phys Rev A (Coll Park), vol. 89, no. 4, p. 042330, Apr. 2014, doi: 10.1103/PhysRevA.89.042330.
[47] M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, N. A. Silva, Secret key rate of multi-ring M-APSK continuous variable quantum key distribution, Optics Express, Vol. 29, No. 23, pp. 38669 - 38669, November, 2021.
[48] A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation," Phys Rev A (Coll Park), vol. 83, no. 4, p. 042312, Apr. 2011, doi: 10.1103/PhysRevA.83.042312.
[49] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching," Phys Rev Lett, vol. 93, no. 17, p. 170504, Oct. 2004, doi: 10.1103/PhysRevLett.93.170504.
[50] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," Quantum, vol. 5, p. 540, Sep. 2021, doi: 10.22331/q-2021-09-13-540.
[51] E. Kaur, S. Guha, and M. M. Wilde, "Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution," Phys Rev A (Coll Park), vol. 103, no. 1, p. 012412, Jan. 2021, doi: 10.1103/PhysRevA.103.012412.
[52] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," Phys Rev A (Coll Park), vol. 84, no. 6, p. 062317, Dec. 2011, doi: 10.1103/PhysRevA.84.062317.
[53] W.-B. Liu et al., "Homodyne Detection Quadrature Phase Shift Keying Continuous--Variable Quantum key Distribution with High Excess Noise Tolerance," PRX Quantum, vol. 2, no. 4, p. 040334, Nov. 2021, doi: 10.1103/PRXQuantum.2.040334.
[54] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous--variable quantum key distribution," Phys Rev A (Coll Park), vol. 81, no. 6, p. 062343, Jun. 2010, doi: 10.1103/PhysRevA.81.062343.
[55] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev Mod Phys, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.
[56] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in Advances in Cryptology — EUROCRYPT '93, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 410–423. doi: 10.1007/3-540-48285-7_35.
[57] G. Limei, R. Qi, J. Di, and H. Duan, "QKD Iterative Information Reconciliation Based on LDPC Codes," International Journal of Theoretical Physics, vol. 59, no. 6, pp. 1717–1729, Jun. 2020, doi: 10.1007/s10773-020-04438-9.
[58] Q. Li, B.-Z. Yan, H.-K. Mao, X.-F. Xue, Q. Han, and H. Guo, "High-Speed and Adaptive FPGA-Based Privacy Amplification in Quantum Key Distribution," IEEE Access, vol. 7, pp. 21482–21490, 2019, doi: 10.1109/ACCESS.2019.2896259.
[59] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans Inf Theory, vol. 41, no. 6, pp. 1915–1923, 1995, doi: 10.1109/18.476316.
[60] A. Stanco et al., "Versatile and Concurrent FPGA-Based Architecture for Practical Quantum Communication Systems," IEEE Transactions on Quantum Engineering, vol. 3, pp. 1–8, 2022, doi: 10.1109/TQE.2022.3143997.
[61] E. O. Samsonov et al., "Vacuum-based quantum random number generator using multi-mode coherent states," Quantum Inf Process, vol. 19, no. 9, p. 326, 2020, doi: 10.1007/s11128-020-02813-3.
[62] X. Guo, C. Cheng, M. Wu, Q. Gao, P. Li, and Y. Guo, "Parallel real-time quantum random number generator," Opt. Lett., vol. 44, no. 22, pp. 5566–5569, Nov. 2019, doi: 10.1364/OL.44.005566.
[63] Z. Lu, J. Liu, X. Wang, P. Wang, Y. Li, and K. Peng, "Quantum random number generator with discarding-boundary-bin measurement and multi-interval sampling," Opt. Express, vol. 29, no. 8, pp. 12440–12453, Apr. 2021, doi: 10.1364/OE.419756.
[64] D. Rusca, H. Tebyanian, A. Martin, and H. Zbinden, "Fast self-testing quantum random number generator based on homodyne detection," Appl Phys Lett, 2020, doi: 10.1063/5.0011479.
[65] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator," Phys Rev Appl, 2021, doi: 10.1103/PhysRevApplied.15.034034.
[66] J. B. Brask et al., "Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination," Phys Rev Appl, 2017, doi: 10.1103/PhysRevApplied.7.054018.
[67] H. Wang et al., "Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area," Commun Phys, vol. 5, no. 1, p. 162, Jun. 2022, doi: 10.1038/s42005-022-00941-z.
[68] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, "Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator." 2023.
[69] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," Appl Phys Rev, vol. 11, no. 1, Mar. 2024, doi: 10.1063/5.0179566.

Nuno Silva licenciou-se em Física pela Universidade do Minho em 2006, e recebeu o grau de mestre em Física pela Universidade de Aveiro em 2008. Doutorou-se em Engenharia Electrotécnica, pela mesma Universidade, em 2013, data a partir da qual colaborou no Instituto de Telecomunicações como bolseiro de pós-doutoramento. Colabora com o Departamento de Física e de Eletrónica, Telecomunicações e Informática ambos da Universidade de Aveiro, onde apoia à lecionação de disciplinas nas áreas da ótica quântica, segurança quântica e tecnologias quânticas. Atualmente, é investigador do Instituto de Telecomunicações, estando inserido no grupo de investigação Optical Quantum Communications, em Aveiro. Ao longo dos anos, participou em mais de 30 projetos de investigação, desenvolvendo conhecimento no domínio da criptografia quântica.

Maurício Ferreira completou o MSc em Engenharia Física em 2021 na Universidade de Aveiro. Atualmente, frequente o programa doutoral em Engenharia Eletrotécnica na mesma instituição e participa no grupo de comunicações quânticas no Instituto de Telecomunicações – Aveiro. O seu trabalho foca-se na implementação de uma plataforma quântica de geração de números aleatórios resiliente a imperfeições experimentais.

Sara Mantey obteve o MSc em Engenharía Física em 2021, na Universidade de Aveiro. Atualmente está a fazer o doutoramento em Engenharia Eletrotécnica na Universidade de Aveiro em parceria com o Instituto de Telecomunicações – Aveiro, no grupo de comunicações quânticas. O seu trabalho foca-se na implementação prática de sistemas quânticos para a distribuição de chaves com codificação na polarização. Os seus interesses principais envolvem comunicações óticas, comunicações quânticas e técnicas de controlo da polarização.

Margarida Almeida obteve o MSc em Engenharia Física pela Universidade de Aveiro em 2021. Atualmente é aluna de doutoramento em Engenharia Electrotécnica na Universidade de Aveiro em parceria com o Instituto de Telecomunicações – Pólo de Aveiro. Iniciou o seu trabalho no Instituto de Telecomunicações em 2018, estando inserida no grupo Optical Quantum Communications and Technologies desde então. Os seus principais interesses envolvem a distribuição quântica de chaves com variáveis contínuas, com foco no pós-processamento necessário para a extração de chaves simétricas, e na sua implementação experimental, principalmente no que diz respeito às imperfeições do sistema.

Gustavo Anjos recebeu o grau de mestre e de doutorado em engenharia elétrica pela Universidade de Aveiro em 2013 e 2022, respectivamente. Ele tem desenvolvido trabalho de investigação no Instituto de Telecomunicações em Aveiro, participando em múltiplos projectos como FLEXICELL, SWING2 e DISCRETION. Actualmente trabalha como investigador no Instituto de Telecomunicações na Universidade de Aveiro desenvolvendo trabalho no grupo de comunicações quânticas. Os seus atuais interesses de investigação incluem segurança ao nível da camada física para comunicações sem fio, e sistemas de distribuição de chaves quânticas. Neste último caso, o foco de trabalho incide na implementação deste tipo protocolos em plataformas de hardware dedicadas tendo em vista a computação eficiente dos algoritmos associados.

Nelson Muga licenciou-se em Física pela Universidade do Porto, em 2002, e recebeu os graus de mestre em Física Aplicada, em 2006, e doutor em Engenharia Física, em 2011, ambos pela Universidade de Aveiro. Fez pós-doutoramento no Instituto de Telecomunicações, colaborando com o Departamento de Física da Universidade de Aveiro desde 2016, onde leciona disciplinas nas áreas da ótica e optoelectrónica. Atualmente, é investigador auxiliar do Instituto de Telecomunicações, estando inserido no grupo de investigação Optical Quantum Communications, em Aveiro. Ao longo dos anos, participou em mais de 30 projetos de investigação, desenvolvendo conhecimento no domínio dos sistemas de comunicação por fibra ótica de elevada velocidade e no domínio das comunicações quânticas. É autor de mais de 150 publicações científicas (50 artigos em revistas internacionais com revisão por pares, 96 atas de conferências, 5 capítulos de livros) e de uma patente.

Armando Nolasco Pinto é Professor Catedrático do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e lidera o grupo de Comunicações Quânticas do Instituto de Telecomunicações em Aveiro. É autor e apresentou seu trabalho em mais de 200 revistas e conferências científicas internacionais. O trabalho por si realizado e pela equipa que coordena foi distinguido com mais de 23 prêmios científicos. Detém 4 patentes internacionais e participou em 57 projetos de investigação, tendo sido coordenador global de 24. Atualmente, é coordenador de um projeto da União Europeia e de um projeto da NATO, ambos na área das tecnologias de comunicação quânticas. É membro do Conselho Editorial das revistas "Scientific Reports", publicadas pela Nature, e das revistas "Optical and Quantum Electronics" e "Quantum Communication", publicadas pela Springer e pelo Institute of Engineering and Technology, respetivamente. É o Presidente da Comissão Técnica de Normalização CTE JTC 22 – Tecnologias Quânticas, a funcionar no âmbito IEP - Instituto Eletrotécnico Português. É membro Sénior do Institute of Electrical and Electronics Engineers e membro Sénior da Optica Society.