

Iniciativa em Redes Quânticas e suas Aplicações no Instituto Tecnológico de Aeronáutica

Edison Puig Maldonado¹, André Jorge Carvalho Chaves¹, Rene Felipe Keidel Spada¹, Marcelo Marques¹, Lara Kühn Teles¹, Tobias Frederico¹, Caio Regis Aguiar Moreira¹, Fausto Batista Mendonça¹, Mateus Habermann¹, Vilson Rosa de Almeida¹, Augusto Ribeiro Rodrigues¹, Ingrid David Barcelos², Romildo Henrique de Souza¹, Lucio Pinheiro Amaro¹, Renato Machado¹

¹Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil

²Laboratório Nacional de Luz Síncrotron (LNLS), Centro Brasileiro de Pesquisa em Energia e Materiais (CNPEM), Campinas /SP – Brasil

Resumo – Docentes do Instituto Tecnológico de Aeronáutica (ITA) uniram-se para ampliar suas ações em tecnologias quânticas, apresentando proposta para expansão da capacidade de pesquisa da instituição nesta área. Objetiva-se maior impacto nas atividades de ensino e pesquisa, no apoio ao desenvolvimento de novas propostas de negócios, contribuindo também para a educação e a popularização de C&T, ao entendimento e uso destas tecnologias pela sociedade brasileira.

Palavras-Chave – sistemas de informação quântica, cibersegurança e criptografia quântica, redes quânticas.

I. INTRODUÇÃO

Princípios da mecânica quântica, teoria fundamental da física, aplicadas ao campo interdisciplinar atualmente denominado “informação quântica”, têm o potencial de revolucionar as telecomunicações, sistemas sensores e a computação [1]. A superposição quântica, o emaranhamento quântico, a não-clonagem e fenômenos tais como o tunelamento têm propiciado recentemente um conjunto de mecanismos, dispositivos e sistemas que podemos denominar “novas tecnologias quânticas” ou TQ [2, 3]. Apesar de ser considerada uma área sensível, produtos comerciais dessas novas tecnologias começam a ser disponibilizados. Empresas de serviços financeiros, telecomunicações, logística, biotecnologia e muitas outras, começam agora a procurar profissionais qualificados em TQ [4].

A capacidade tecnológica para realizar conexões de dados quânticos representa um requisito de qualificação para TQ. O domínio e implementação de técnicas de criptografia quântica nestas conexões, objetivo estratégico para muitos países, governos e empresas, movimentam um novo mercado nessa área. Técnicas de troca de chaves criptográficas em enlace quântico, ou QKD [5, 6], possibilitam uma camada de proteção física que, em condições ideais, garante segurança contra diversos ataques, inclusive potenciais ataques que utilizem computadores quânticos [7].

Além disso, prevê-se que novos sensores quânticos permitirão em curto prazo avanços significativos em áreas da pesquisa científica, em metrologia, em técnicas de radar, em imageamento médico, em visualização topológica (incluindo subterrâneos) e monitoramento ambiental [3]. Por outro lado,

simuladores quânticos (sistemas quânticos controláveis que podem ser usados para simular outros sistemas quânticos) permitem resolver problemas científicos que não são tratáveis por outros meios, por exemplo, modelar as propriedades quânticas de partículas, resolvendo assim problemas relevantes para a ciência de materiais e química, dentre outros [8]. A computação quântica (QC) pode resolver novos problemas e facilitar a integração de informações industriais, tal como em computação intensiva para análise de dados. Porém, este campo ainda enfrenta muitos desafios, dentre os quais problemas de decoerência quântica, instabilidades de qubits (sensibilidade a ruídos e interferências), problemas de escalabilidade, altos requisitos de recursos e tecnologia de circuitos ainda em desenvolvimento [9], portanto ainda não permitindo muitas aplicações práticas [10].

Este quadro traz novos desafios para as instituições do país. Requer, nesse estágio inicial da área no Brasil enquanto tecnologia, o trabalho conjunto intensivo do estado da arte de ciência e engenharia brasileiras. O Instituto Tecnológico de Aeronáutica, ITA, é uma instituição tradicional brasileira que conta em sua Divisão de Engenharia Eletrônica com o Laboratório de Guerra Eletrônica – LAB-GE [11], sendo este uma importante referência nacional em pesquisa acadêmica nas áreas de fotônica, materiais eletromagnéticos, radar e outros sistemas em RF e micro-ondas, sensores e comunicação segura – foi criado em 2001 para apoiar o ensino e a pesquisa em áreas de interesse da Defesa, o Curso de Especialização em Análise de Ambiente Eletromagnético (CEAAE) e o Programa de Pós-graduação em Aplicações Operacionais (PPGAO). Além disso, o ITA possui uma pós-graduação em física muito tradicional no país (<https://www.pgfis.ita.br/>), com o início das suas atividades na década de 1960 [12], e atualmente conta com um corpo docente atuante em nanotecnologia, nanofotônica e sistemas quânticos. Assim, o ITA possui importantes competências para atuar nesse campo transversal e uma cultura de dedicação a projetos aplicados, os quais poderão atender a demandas da sociedade brasileira.

Esse trabalho apresenta aspectos da iniciativa em implementação no ITA para uma nova infraestrutura de pesquisa em conexões de dados quânticos, voltada à comunicação segura, objetivando viabilizar novos estudos, projetos, cursos e treinamentos. Esta conta já com espaços físicos específicos, um grupo de pesquisadores associados, financiamento e apoio institucional.

E. P. Maldonado, puig@ita.br. Este trabalho é parcialmente financiado por Financiadora de Estudos e Projetos – FINEP, vinculada ao Ministério da Ciência, Tecnologia e Inovação, através do Projeto 0734/24.

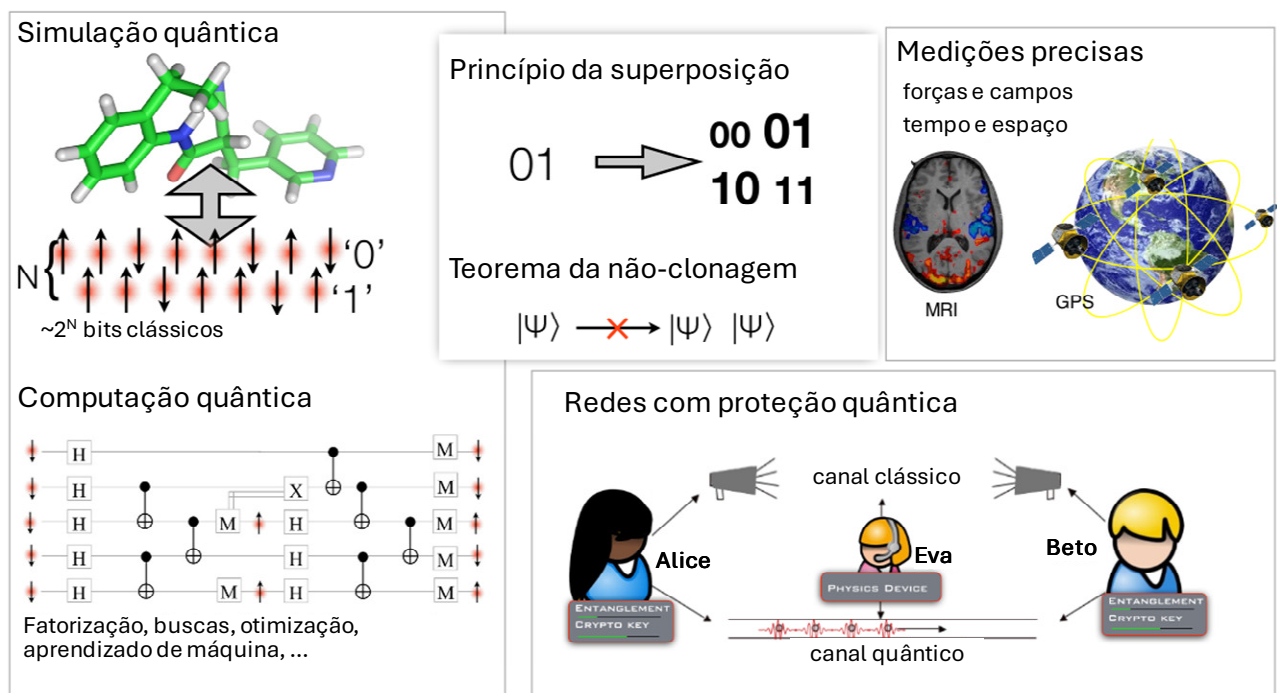


Fig. 1. Áreas principais das novas tecnologias quânticas: simulação quântica, computação quântica, sensores e metrologia quântica, comunicações quânticas (traduzido de "Future Directions of Quantum Information Processing" [13]).

II. APLICAÇÕES E USO DUAL

O progresso nas novas tecnologias quânticas na comunicação, na detecção/metrologia e na computação acelerou acentuadamente nos últimos anos, impulsionado por melhorias em tecnologias de fabricação, detecção e controle, além de avanços na teoria da informação quântica, com novos algoritmos, técnicas e protocolos [13]. A Figura 1 mostra três áreas principais: simulação e computação quântica, sensores quânticos e comunicações quânticas, todas consistindo em avanços e capacidades inéditas, possibilitadas pelas leis da mecânica quântica e pelas propriedades dos estados quânticos.

Muitas das aplicações destas novas tecnologias são de dupla utilização ou são utilizadas diretamente para fins militares e pode-se esperar que apresentem impactos estratégicos e de longo prazo. As aplicações militares de TQ não só oferecerão melhorias e novas capacidades, mas também exigirão o desenvolvimento de novas estratégias, táticas e políticas, avaliação de ameaças à paz e segurança globais e identificação de questões éticas. Considerando a escala TRL (*technology readiness level*) de níveis de maturidade tecnológica, definidos para estimar o estado de desenvolvimento e disponibilidade a aplicações, de 1 a 9, as novas tecnologias quânticas individuais estão em grande parte em TRLs iniciais (princípios básicos observados) até TRL 6 (tecnologia demonstrada em ambiente relevante). Destaca-se, entretanto, a tecnologia QKD (*quantum key distribution*), inclusive para conexões com satélites, com TRL entre 7 e 8, já com diversos sistemas instalados e expectativa de impacto completo em poucos anos [14].

Previsões precisas sobre a implantação destas tecnologias não são possíveis, uma vez que a transição do estudo em laboratório para aplicações reais em muitos casos ainda não foi iniciada ou está em curso; ainda assim, especialistas consideram que o conhecimento em TQ deve ser cultivado no ambiente militar, de forma a monitorar de perto o seu desenvolvimento e emprego [14].

III. UMA PROPOSTA DE EXPANSÃO EM PESQUISA

Juntamente com docentes da Divisão de Engenharia Eletrônica (IEE) e do Departamento de Física da Divisão de Ciências Fundamentais (IEF), o LAB-GE decidiu que deveria articular um crescimento das atividades na área de TQ no ITA, em pesquisa científica e tecnológica, experimental e por modelos, desenvolvimentos e aplicações, também nas áreas educacional, de extensão e de serviços. Elegeram-se como meta inicial a expansão de infraestrutura e a implementação no ITA de enlaces de dados quânticos em fibra óptica (OFC) e no espaço livre (FSO), operando em protocolos QKD.

Em seu Plano de Desenvolvimento Institucional (PDI) [15], o ITA define duas linhas de pesquisa prioritárias às quais a criação de um núcleo de excelência em pesquisa em TQ exibe aderência: a linha "Comando e controle, guerra eletrônica e segurança cibernética" e a linha "Pesquisa em Física, Química e Matemática". A característica contemporânea e predominantemente aplicada de uma expansão da infraestrutura de pesquisa em TQ terá também significativo impacto positivo no ensino de pós-graduação, com potencial para subsidiar novas disciplinas e atividades de

pesquisa, em especial nos seguintes programas: 1) programa PG/EEC, na área de Engenharia Eletrônica, 2) programa PG/FIS, na área de Física, 3) programa PPGAO, voltado a aplicações em Defesa. Demandas de cursos e treinamentos específicos, de órgãos governamentais, instituições e empresas brasileiras em geral também passarão a poder ser atendidas.

Esta iniciativa está também em consonância com a Política de Inovação oficial do ITA (PI), buscando a modernização do ensino e sua excelência, a formação de profissionais atualizados com as temáticas do setor produtivo e da sociedade, buscando oferecer à sociedade soluções para projetos-piloto, propostas experimentais e capacitação. Em específico, este projeto representa implementação de várias políticas de inovação do ITA.

Outros projetos em TQ deverão ser propostos por docentes e pesquisadores do ITA nos próximos anos, por exemplo na área de sensoriamento quântico. Dadas as dimensões territoriais brasileiras e a grande quantidade de áreas para serem monitoradas (como a Amazônia), as tecnologias quânticas de sensoriamento ambiental se mostram também como uma oportunidade futura para as competências que serão criadas com esse projeto, em especial para a Força Aérea Brasileira.

Os resultados destas ações deverão também propiciar maiores oportunidades de inovação tecnológica, permitindo a empresas brasileiras oferecer sistemas e produtos tecnologicamente novos e/ou aprimorados, assim como novos serviços na área.

IV. CARACTERÍSTICAS DA PROPOSTA

Sistemas de comunicação contendo um canal quântico deverão ser disponibilizados à sociedade brasileira para testes de regimes de operação, testes de componentes, pesquisa de novas técnicas, treinamentos e demonstrações. Estas implementações terão como objetivo propiciar ao ITA maior produção em pesquisa, desenvolvimento e formação de recursos humanos nas aplicações de redes de dados quânticos voltados à comunicação segura, comando, controle e segurança cibernética e à defesa. A nova infraestrutura estará centralizada em um novo espaço de pesquisa experimental em fotônica para TQ no LAB-GE, com a instalação de conjunto de novos equipamentos de enlaces protegidos por QKD, seguindo alguns dos principais protocolos atualmente em uso, com características para uso acadêmico e científico nesta área e gestão multiusuário. Além disso, incluirá a implementação de um novo cluster de computação de alto desempenho, o qual permitirá ao ITA expandir estudos de processos e dispositivos avançados em TQ pela equipe do projeto e colaboradores.

Este é um projeto na fronteira do conhecimento tecnológico, particularmente baseada na área de fotônica e optoeletrônica, e em materiais e técnicas em física de estado sólido, em especial, materiais bidimensionais. A equipe atual

desse projeto apresenta-se com alta qualificação, experiência e competência para sua execução, um time com especialidades complementares e trabalhos de impacto já realizados em fotônica e em telecomunicações, em dispositivos quânticos e em computação quântica.

A. Resultados esperados para o ITA

Do ponto de vista institucional, estas ações deverão resultar nas seguintes conquistas:

1) A implementação do espaço multiusuário para o estudo experimental de enlaces de dados quânticos poderá colocar o ITA entre as primeiras instituições a disponibilizar esta infraestrutura à sociedade brasileira, apoiando assim a pesquisa e a inovação nesta área de forma disseminada.

2) A disponibilização de novo cluster de computação de alto desempenho permitirá novos estudos em materiais e dispositivos para TQ e assim resultados de maior impacto.

3) A formação de um time de pesquisadores do ITA que irá colaborar em pesquisas nesse campo, projeta o início de um ciclo virtuoso de aumento do conhecimento, a formação de um núcleo de especialistas nessa região do Estado de SP.

B. Resultados esperados para a sociedade

Com relação à sociedade brasileira, estas ações deverão resultar especialmente nos seguintes avanços:

1) A oferta de capacidade técnica que irá impactar positivamente em novas propostas de negócios nesta área, realizadas por empresas brasileiras.

2) A formação de novos recursos humanos especializados em TQ, em especial na pós-graduação, mas também atendendo a demandas da FAB, da sociedade brasileira, de instituições e empresas.

V. SISTEMAS E GESTÃO DOS NOVOS RECURSOS

Os novos recursos de computação de alto desempenho serão disponibilizados no já existente Laboratório de Computação Científica Avançada e Modelamento do ITA – LAB-CCAM. Consistirão em um ou mais novos servidores de computação de alto desempenho (>100 núcleos, ~512 GB de memória, armazenamento da ordem de 50 TB), em um novo data center com toda a infraestrutura necessária modernizada.

No LAB-GE, será criado um laboratório de pesquisa experimental em implementações fotônicas de TQ, o *Espaço ITA de Tecnologias Quânticas* (EQ), sob a responsabilidade de uma equipe de pesquisadores da Divisão de Engenharia Eletrônica do ITA. O público-alvo pretendido visa a usuários (em geral, cientistas e engenheiros) do ITA, do DCTA, de outros setores da FAB, de instituições das áreas de defesa,

segurança e ciência e tecnologia dos governos federal, estaduais e municipais, de outras ICTs públicas ou privadas, assim como de empresas brasileiras. Propostas serão selecionadas conforme avaliação nas dimensões: 1) relevância científica, tecnológica, educacional, social e econômica; 2) impactos esperados; 3) potencial de inovação; 4) formação de recursos humanos. Será assegurada a igualdade de oportunidades a empresas e demais organizações interessadas. Projetos apoiados deverão preferencialmente utilizar recursos do EQ de forma compartilhada simultânea e apresentar execução no menor intervalo de tempo. Somente em casos excepcionais projetos poderão ocupar todo o ambiente do EQ e impor restrição de acesso. Acordos poderão abranger: a) pesquisa científica, aplicada ou tecnológica, b) extensão, c) desenvolvimento de protótipos para avaliação, teste ou demonstração, d) criação de novos produtos, serviços, processos ou aprimoramento dos existentes, d) capacitação, formação e aperfeiçoamento de RH. A gestão de cada acordo deverá utilizar uma Fundação de Apoio como interveniente e executora financeiro-administrativa.

Comitê Gestor

O Comitê Gestor (CG) terá o papel de órgão executivo responsável pela operação do EQ e pela definição de suas políticas. Será composto pelo Chefe do IEE, pelo Gestor e pelo Adjunto do LAB-GE, além do Coordenador do EQ.

O CG se reunirá periodicamente para execução de suas atividades, em especial para aprovação de cronogramas e acompanhamento de resultados. Deliberações serão comunicadas a usuários e interessados através do sítio Web do LAB-GE. Terá como atribuições:

- A gestão de equipamentos (de uso livre ou restrito).
- Organização da seleção de projetos e da agenda de uso.
- Definição de plano de ação com recomendações para o a alocação de tempo destinadas modalidades específicas de projetos, assim como de prestações de serviços.
- Definição de políticas de alocação de uso tendo como orientação o Art. 4º da Lei nº. 10.973, de 2 de dezembro de 2004 (Lei da Inovação).

VI. OBSERVAÇÕES FINAIS

Uma nova infraestrutura de pesquisa irá permitir ao ITA a realização de estudos e projetos de maior impacto no estado da arte na área de conexões de dados quânticos voltados à comunicação segura, também para aplicações de defesa, comando e controle, guerra eletrônica e segurança cibernética. Consistirá em um laboratório de pesquisa experimental em fotônica, no Laboratório de Guerra Eletrônica – LAB-GE, que será equipado e terá expansão de atividades para ser capacitado a estudos na área de informação quântica.

A capacitação na área de enlaces de dados quânticos contribui positivamente na viabilização de futuros projetos. O LAB-GE pretende dar continuidade à sua atuação em TQ com projetos que contemplem:

1) A ampliação do escopo da pesquisa e desenvolvimento para a área de redes quânticas e a internet quântica.

2) A possibilidade de desenvolvimento comunicação segura com satélites, com proteção quântica, o que colocaria o Brasil entre as poucas nações do mundo com esta tecnologia.

3) Desenvolvimentos em tecnologias de sensores quânticos e na engenharia destes sistemas.

O estudo de novos processos, materiais, componentes e dispositivos utilizáveis nas novas tecnologias quânticas será potencializado pela expansão do Laboratório de Computação Científica Avançada e Modelamento – LAB-CCAM.

A formação de um grupo de professores especialistas colaboradores também irá propiciar maior atividade e impacto em ações do ITA nas áreas das novas tecnologias quânticas, e de forma imediata, proporcionar novos cursos e treinamentos, novas atividades de desenvolvimento e de pesquisa em nível de pós-graduação em tecnologias de dados quânticos no ITA.

AGRADECIMENTOS

C. R. A. M. agradece o apoio parcial do Instituto Nacional de Ciência e Tecnologia (INCT-Sinais), financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) sob bolsa 406517/2022-3. I. D. B. agradece ao CNPq, proc. 408144/2022-0. R. F. K. S agradece à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), proc. 2019/07671-4, e ao CNPq, proc. 405562/2022-5, 307846/2021-0 e 423423/2021-5. T. F. agradece à FAPESP, proc. 2019/07767-1, e ao CNPq, proc. 306834/2022-7. V. R. A. agradece ao CNPq, proc. 306389/2021-5 e 403031/2019-2.

REFERÊNCIAS

- [1] U.S. DEPARTMENT OF ENERGY. Report of the DOE Quantum Internet Blueprint Workshop. [S. l.: s. n.], 2020. Available at: https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf.
- [2] GIBNEY, Elizabeth. Quantum gold rush: the private funding pouring into quantum start-ups. *Nature*, vol. 574, no. 7776, p. 22–24, 3 Oct. 2019. <https://doi.org/10.1038/d41586-019-02935-4>.
- [3] KANTSEPOLSKY, Boris; AVIV, Itzhak; WEITZFELD, Roye; BORDO, Eliyahu. Exploring Quantum Sensing Potential for Systems Applications. *IEEE Access*, vol. 11, p. 31569–31582, 2023. <https://doi.org/10.1109/ACCESS.2023.3262506>.
- [4] CHEN, Sophia. The future is quantum: universities look to train engineers for an emerging industry. *Nature*, vol. 623, no. 7987, p. 653–655, 16 Nov. 2023. <https://doi.org/10.1038/d41586-023-03511-7>.

- [5] PIRANDOLA, S.; ANDERSEN, U. L.; BANCHI, L.; BERTA, M.; BUNANDAR, D.; COLBECK, R.; ENGLUND, D.; GEHRING, T.; LUPO, C.; OTTAVIANI, C.; PEREIRA, J.; RAZAVI, M.; SHAARI, J. S.; TOMAMICHEL, M.; USENKO, V. C.; VALLONE, G.; VILLORESI, P.; WALLDEN, P. *Advances in Quantum Cryptography. Advances in Optics and Photonics*, vol. 12, no. 4, p. 1012, 31 Dec. 2020. <https://doi.org/10.1364/AOP.361502>.
- [6] GYONGYOSI, Laszlo; BACSARDI, Laszlo; IMRE, Sandor. A Survey on Quantum Key Distribution. *Infocommunications journal*, vol. 11, no. 2, p. 14–21, 2019. <https://doi.org/10.36244/ICJ.2019.2.2>.
- [7] LAI, Junsen; YAO, Fei; WANG, Jing; ZHANG, Meng; LI, Fang; ZHAO, Wenyu; ZHANG, Haiyi. Application and Development of QKD-Based Quantum Secure Communication. *Entropy*, vol. 25, no. 4, p. 627, 6 Apr. 2023. <https://doi.org/10.3390/e25040627>.
- [8] ALTMAN, Ehud; BROWN, Kenneth R.; CARLEO, Giuseppe; CARR, Lincoln D.; DEMLER, Eugene; CHIN, Cheng; DEMARCO, Brian; ECONOMOU, Sophia E.; ERIKSSON, Mark A.; FU, Kai-Mei C.; GREINER, Markus; HAZZARD, Kaden R.A.; HULET, Randall G.; KOLLÁR, Alicia J.; LEV, Benjamin L.; LUKIN, Mikhail D.; MA, Ruichao; MI, Xiao; MISRA, Shashank; ... ZWIERLEIN, Martin. Quantum Simulators: Architectures and Opportunities. *PRX Quantum*, vol. 2, no. 1, p. 017003, 24 Feb. 2021. <https://doi.org/10.1103/PRXQuantum.2.017003>.
- [9] SOOD, Sandeep Kumar; POOJA. Quantum Computing Review: A Decade of Research. *IEEE Transactions on Engineering Management*, vol. 71, p. 6662–6676, 2024. <https://doi.org/10.1109/TEM.2023.3284689>.
- [10] LU, Yang; SIGOV, Alexander; RATKIN, Leonid; IVANOV, Leonid A.; ZUO, Min. Quantum computing and industrial information integration: A review. *Journal of Industrial Information Integration*, vol. 35, p. 100511, Oct. 2023. <https://doi.org/10.1016/j.jii.2023.100511>.
- [11] LAB-GE, Laboratório de Guerra Eletrônica, <https://www.ele.ita.br/~labge/>
- [12] APG-ITA, Associação de Pós-Graduandos do Instituto Tecnológico de Aeronáutica História da Pós-Graduação no ITA, https://apgita.org.br/wp-content/uploads/2019/08/HISTORIA_DA_POS_GRADUACAO.pdf
- [13] LLOYD, Seth; ENGLUND, Dirk. *Future Directions of Quantum Information Processing*. VT-ARC. [S. l.]: Virginia Tech, 2017.
- [14] KRELINA, Michal. Quantum technology for military applications. *EPJ Quantum Technology*, vol. 8, no. 1, p. 24, 6 Dec. 2021. <https://doi.org/10.1140/epjqt/s40507-021-00113-y>.
- [15] Instituto Tecnológico de Aeronáutica, “Visão e Futuro - Plano de Desenvolvimento Institucional 2021-2023”. [Online]. Disponível em: <http://www.ita.br/pdi>