SEGURANÇA DA INFORMAÇÃO EM TELECOMUNICAÇÕES AERONÁUTICAS: DISCUSSÃO DA VIABILIDADE E BENEFÍCIOS DA UTILIZAÇÃO DE CRIPTOGRAFIA QUÂNTICA

Carlos Henrique A. Costa
João Batista Camargo Jr.
Grupo de Análise de Segurança - GAS
Escola Politécnica da USP

RESUMO
A importância que canais de dados vêm adquirindo para a telecomunicação aeronáutica tem feito com que requisitos de segurança da informação se tornem um aspecto relevante para manutenção da segurança na operação aérea. Considerando o caso de veículos aéreos não-tripulados este aspecto se torna ainda mais crucial. Tradicionalmente tais requisitos são alcançados com a utilização de métodos de criptografia clássica. Contudo, devido à segurança desses serem fundamentada na dificuldade de solução de problemas matemáticos não demonstrada e com o surgimento da computação quântica, tem-se apontado grandes fragilidades para essa forma de criptografia. Este trabalho tem como objetivo analisar a viabilidade de utilização da nova técnica de criptografia quântica na telecomunicação aeronáutica e os benefícios que esta pode proporcionar, especialmente na operação de veículos aéreos não-tripulados.

ABSTRACT
The role that Data Links has acquiring in aeronautical telecommunications leads the information security requirements assumes an important function to keep the safety of aerial operation. Considering the case of unmanned aerial vehicles this aspect becomes more crucial. Traditionally, the utilization of classical cryptographic methods satisfies these requirements. However, the fact that security base of classical methods be represented by mathematical problems solution difficulty that isn't appropriately demonstrated and the quantum computing sprouting raise great fragilities to classical cryptography. The aim of this work is to analyze the benefits that new quantum cryptography technique utilization in an aeronautical telecommunications scenario can promote, especially in the unmanned aerial vehicles operation.

1. INTRODUÇÃO

Os benefícios da comunicação digital entre ar e solo para provimento de informações gráficas de posicionamento, dados de vôo, estado e outros intensificaram a ocorrência de canais de dados na telecomunicação aeronáutica, sendo o movimento para a consolidação da *Aeronautical Telecomunication Network (ATN)* um reflexo importante desse processo. O aumento de funções de uma aeronave controladas por esse meio tem levado a uma crescente preocupação com a segurança dos dados de comunicação aeronáutica, sendo o documento de práticas recomendadas e padrões produzido pela ICAO (ICAO, 2002) para o tratamento de ameaças e vulnerabilidades em redes aeronáuticas um bom compêndio disso. Esse quadro se torna crítico nos veículos aéreos não-tripulados, onde toda a informação de controle e tráfego de dados é transmitida digitalmente, fazendo com que nesse cenário uma falha no âmbito dos dados possa gerar graves acidentes. A crescente utilização de veículos não-tripulados e sua futura operação civil em conjunto com aeronaves tripuladas em um ambiente comercial e utilizando uma rede padrão para comunicação de dados em aeronaves e a intensificação do uso dessa rede por aeronaves convencionais tornam os aspectos de segurança de dados estratégicos para o setor.

A atual implementação da *ATN* busca satisfazer requisitos de segurança da informação utilizando algoritmos clássicos de distribuição de chaves criptográficas para autenticação de mensagens e verificação de autenticidade de dispositivos móveis e fixos na rede (McMath, J., 2003). A principal fragilidade desse sistema abordada aqui é o fato dos protocolos criptográficos clássicos não possuírem uma demonstração formal de que a base de sua segurança é inviolável. Esses métodos estão fundamentados no dado empírico da intratabilidade computacional da solução de alguns problemas matemáticos em tempo viável, sendo, no entanto, que uma demonstração matemática para esse fato ainda não foi obtida. Isso torna possível a existência de uma vulnerabilidade que é desconhecida, ou em uma situação pior, conhecida por algum grupo que não tornou esse fato público. Um segundo agravante são os novos métodos de tratamento da informação representado pelos computadores quânticos. Apesar da área ainda estar em seu estágio inicial, já é conhecido e demonstrado que para computadores que utilizam essa tecnologia a solução dos problemas centrais dos atuais métodos de criptografia é alcançada em tempo viável. Em ambos os casos, a segurança dos sistemas criptográficos clássicos, por conseguinte, toda comunicação que se utiliza desses estaria seriamente vulnerável.

A criptografia quântica consiste em um método criptográfico cuja segurança se fundamenta em propriedades físicas, ou seja, na impossibilidade da violação destas, tornando-o incondicionalmente inviolável. Essa técnica tem recebido grande atenção em todo mundo devido aos diversos benefícios que pode gerar em termos de segurança de dados em redes de telecomunicações. Simultaneamente as formas de implementação de protocolos quânticos vêm se tornando mais confiáveis e viáveis com a evolução da tecnologia fotônica. Com isso, atualmente cresce o número de realizações bem sucedidas de criptografia quântica em situações cada vez mais freqüentes e as aplicações do método estão se diversificando. Claramente os benefícios da utilização dos métodos criptográficos quânticos têm um forte impacto positivo nas telecomunicações aeronáuticas, sendo que o atual estágio da tecnologia permite a análise da integração dessa técnica na estrutura existente atualmente.

Este trabalho apresenta um panorama geral da viabilidade da utilização de protocolos de criptografia quântica na telecomunicação aeronáutica nos moldes atuais e considerando as recomendações dos órgãos regulamentadores. A seção 2 apresenta os principais problemas de segurança da informação encontrados em redes aeronáuticas e os riscos que geram para a operação aérea de veículos tripulados e especialmente veículos não-tripulados. Na seção 3 a técnica de criptografia quântica é tratada mais formalmente e é avaliado o principal protocolo quântico atual e seus benefícios. A seção 4 analisa a utilização de criptografia quântica em um cenário realista e discute os principais problemas a serem solucionados para a utilização em ambiente comercial. A última seção apresenta as conclusões do trabalho.

2. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO EM TELECOMUNICAÇÕES AERONÁUTICAS

Sendo a transmissão de dados em aeronáutica responsável principalmente pela comunicação numérica entre estações de solo e aeronaves para provimento de informações de controle e navegação, as principais ameaças de segurança da informação podem ser classificadas em três classes principais:

- Monitoração – Por meio da monitoração do canal de dados uma terceira parte pode adquirir informação sobre o vôo, tráfego, posição e outros. Os canais de dados atuais não garantem a privacidade da informação trafegada
- *Spoofing* – A monitoração do canal pode permitir que uma terceira parte adquira informações de autenticação e assim consiga personificar uma das partes da comunicação
- Modificação – Com a personificação das partes da comunicação é possível que se entre no caminho dos dados. A integridade da informação não é mais garantida neste caso e pode ser corrompida sem que isso seja identificado.

Os requisitos de segurança de dados para a rede *ATN* propostos pela edição 3 da recomendação *ICAO ATN SARPs 9705* (ICAO, 2002) são:

- A *ATN* necessita de um mecanismo flexível para estabelecimento e atualização segura de chaves privadas no contexto de segurança da informação em canais de dados
- O mecanismo de segurança da *ATN* necessita suportar uma Infra-estrutura de chaves públicas (*ICP*)
- É necessário o estabelecimento e atualização segura de chaves públicas para aeronaves e outros dispositivos aviônicos

Esses requisitos de segurança são satisfeitos atualmente utilizando os protocolos de criptografia de chaves públicas para distribuição de chaves, principalmente algoritmo RSA e algoritmo de curvas elípticas – fundamentados respectivamente na dificuldade computacional da fatoração de números inteiros grandes e a solução de funções de curvas elípticas – para realização de autenticação por assinatura digital e função de *hash*. A hipótese do método consiste em que para uma chave criptográfica suficientemente grande, a solução do algoritmo não pode ser realizada em tempo viável com computação tradicional, ao menos que se possua a respectiva chave privada. Formalmente, os métodos RSA e de curvas elípticas consideram que o tempo necessário para quebrar o método cresce exponencialmente com o tamanho da chave. Contudo, não foi realizada ainda uma prova formal que não existe um algoritmo mais eficiente para o tratamento da fatoração de inteiros ou solução de funções de curvas elípticas por computadores clássicos.

O desenvolvimento de novas técnicas de manipulação de informação por sistemas físicos criou o conceito de computação quântica. Dispositivos desse tipo manipulam dados utilizando partículas elementares como elétrons e fótons, beneficiando-se de novas propriedades existentes para a física dessa dimensão. A despeito das dificuldades de implementação ainda existentes para os computadores quânticos, já foi demonstrado que estes

tratam da complexidade computacional de uma forma totalmente inédita. Alguns resultados importantes para questões de segurança da informação nos moldes atuais já foram demonstrados. É conhecido que um computador quântico consegue tratar em tempo hábil o problema da fatoração de inteiros e a solução de curvas elípticas, fazendo isso em tempo polinomial com o tamanho da chave. Além disso, foi também demonstrado que um computador quântico pode realizar a busca de elementos em uma seqüência arbitrária, problema que constitui o núcleo de outros métodos de criptografia clássica devido a sua dificuldade de solução para computadores tradicionais, também em tempo polinomial.

A segurança de sistemas criptográficos depende de todos os elementos do sistema. Dessa forma uma violação em qualquer uma das partes do mecanismo atual de distribuição de chaves públicas tornaria o sistema vulnerável como um todo. É importante ressaltar que não há, no entanto, nenhuma garantia que, mesmo na ausência de computadores quânticos, não haja uma forma de violar os protocolos de criptografia de chave pública.

2.1. Impactos decorrentes de violação da segurança dos dados em comunicações aeronáuticas

A fragilidade dos sistemas criptográficos atuais potencializa uma possível invasão na transmissão de informações aeronáuticas. A aquisição de informações de vôo e a possibilidade de modificação de dados por um indivíduo mal intencionado criam novos estados de risco de acidentes para operação de aeronaves com a possível geração de falhas intencionais. A inevitável intensificação da utilização de canais de dados e diminuição da interferência humana tornam esses riscos ainda maiores.

Os veículos aéreos não-tripulados representam o caso extremo de autonomia de interferência humana e de utilização de canais de dados. Independentemente da classe do veículo, seja controlado remotamente ou de ação autônoma e colaborativa, há somente comunicação realizada por meio digital. Assim, a ação de um veículo não-tripulado está totalmente condicionada a informação que é transmitida pelo canal de dados. Considerando a intensificação das funções exercidas por veículos não-tripulados, de ferramentas de localização e reconhecimento de terrenos, agente militar de ataque a transporte civil de cargas, uma invasão do canal de dados permitiria, em casos extremos, a um invasor desde a aquisição de informação privilegiada, controle indevido de arsenal militar ou apropriação indevida da aeronave, a destruição de carga comercial dentre outras situações perigosas.

Os impactos resultantes da quebra da segurança da informação em comunicação aeronáuticas deixam evidente a relevância da utilização de mecanismos que garantam a não violação dos dados no contexto de uma rede conjunta de operação de aeronaves tripuladas e não-tripuladas, com a possibilidade de distribuição de chaves seguras para os componentes da rede.

3. UTILIZAÇÃO DE CRIPTOGRAFIA QUÂNTICA EM TELECOMUNICAÇÕES

A transmissão de informação pode ser bastante beneficiada pelas intrigantes propriedades apresentadas por sistemas representados por fótons manipulados individualmente, ocorrendo a existência de fenômenos inéditos que aplicados à transmissão de informação se mostram revolucionários. Os fenômenos quânticos têm sido demonstrados com grande precisão e os primeiros dispositivos que se beneficiam das propriedades quânticas passaram a ser construídos na última década. As principais características que fazem com que a utilização de sistemas quânticos na transmissão de informação seja vantajosa são principalmente a existência da limitação física para medição de certas grandezas, fazendo com que sinais quânticos sejam invariavelmente alterados quando ocorre qualquer tipo de interferência. A impossibilidade de não se alterar um sinal quântico dada uma interferência leva a um teorema que é utilizado como um dos fundamentos para transmissão quântica segura. O teorema da não-clonagem (Gobby, C. *et al.,* 2006) estabelece que é impossível copiar um sinal quântico sem alterar de forma significativa o sinal original. Essa propriedade juntamente com a impossibilidade de medição simultânea de estados quânticos não-ortogonais formam os fundamentos desse novo método de criptografia.

A criptografia quântica se apresenta como um método de distribuição de chaves incondicionalmente seguro mesmo quando o invasor possua capacidade tecnológica ilimitada. O protocolo de criptografia quântica proposto em 1984 por C. Bennett e G. Brassard (C. Bennett, C. e Brassard, G., 1984) utiliza fótons polarizados como unidade básica para transmissão de dados. Esse sistema tem se mostrado bastante útil em situações onde a segurança da informação em telecomunicações é um aspecto crítico e vem sendo implementado com grande sucesso por diversos grupos. O fato da segurança da rede governamental *DARPA Quantum Network* (Elliott, C., 2002) ser garantida pelo protocolo é um exemplo da viabilidade de sua utilização.

3.1. Protocolo Bennett-Brassad: BB84

O protocolo é um método criptográfico de distribuição de chaves de sessão ou chaves de uso único e utiliza um canal quântico e um canal clássico, onde é transmitida informação privada e pública respectivamente. O método possibilita uma alta probabilidade de que qualquer pequena interferência na comunicação seja percebida. A principal demonstração de sua segurança contra a ação de um invasor é apresentada no trabalho (Mayers, D., 2001).

O sistema utiliza fótons polarizados em direções ortogonais, considerando os ângulos de polarização de 0, 90 e 45 , 135 graus para estabelecer duas bases para codificar bits – figura 1 – e criando um método que baseado nas regras da mecânica quântica não permite que um invasor possa obter qualquer informação sem alterar de forma significativa o comportamento do sistema. O método consiste em uma forma segura de se estabelecer uma chave de sessão mesmo quando um invasor possua tecnologia avançada ou mesmo capacidade computacional ilimitada uma vez que a segurança do protocolo se fundamenta na violação de leis físicas.

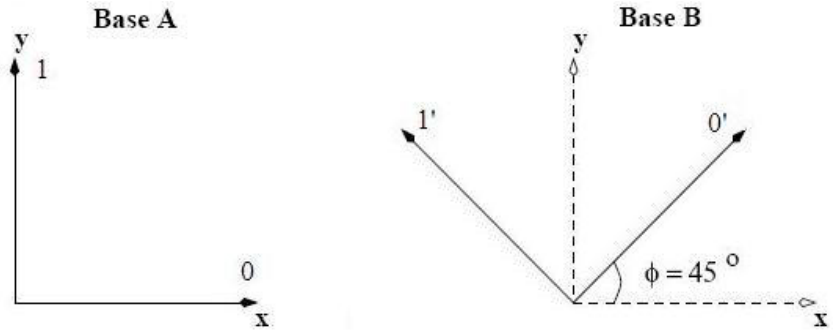


Figura 1: Bases de codificação para polarização de fótons no protocolo BB84

Os fótons polarizados podem ser obtidos a partir de feixes de luz e filtros ou cristais polarizadores. A tecnologia atual consegue produzir LEDs e lasers capazes de emitir um único fóton, possibilitando a emissão de fótons polarizados de acordo com uma direção específica do polarizador. Obtendo um aparato que permita produzir fótons polarizados em duas bases distintas, polarização retilínea (*Base A*) e polarização diagonal (*Base B*), respectivamente 0 e 90 graus e 45 e 135 graus, gerando então, de acordo com a estrutura matemática da mecânica quântica, um sistema em que um fóton polarizado em uma base quando medido em outra base não revelará informação alguma sobre seu estado original. Esse resultado representa o núcleo da segurança do protocolo BB84, já que implica que no caso de um invasor interferir no sinal quântico será produzido um ruído que é facilmente detectado.

O protocolo pode ser descrito resumidamente em termos da linguagem corrente em criptologia pelos passos:

1. Alice gera uma seqüência de *4n* bits aleatórios que codifica utilizando uma das bases linear (*Base A*) ou diagonal (*Base B*) e transmite uma seqüência de fótons a Bob
2. Bob escolhe aleatoriamente a base em que quer realizar a medida e a executa para o conjunto de fótons recebidos
3. Após tal operação Bob utiliza o canal público para anunciar a finalização do processo e a escolha que fez para as bases
4. Alice indica quais escolhas Bob realizou corretamente, ou seja, onde mediu os bits enviados adequadamente. Considerando uma seqüência longa de bits, Bob obterá aproximadamente *2n* bits corretos
5. Alice e Bob compartilham *n* bits da seqüência para realizar a verificação de erros, sendo que qualquer tentativa de invasão será detectada com a presença de uma taxa de erro maior que um patamar aceitável
6. Havendo concordância, Alice e Bob compartilham uma seqüência de bits única que é então utilizada como chave de seção para realização da comunicação

Na figura 2 é mostrado um exemplo de negociação de chave criptográfica quântica utilizando o protocolo BB84.

Seqüência Aleatória de Alice	0	1	1	0	0	0	1	1	0	1	0	1
Escolha de bases de Alice	A	A	B	A	A	B	A	A	B	A	B	B
Bits enviados a Bob	0	1	1'	0	0	0'	1'	1'	0'	1	0'	1'
Escolha de Bases de Bob	A	B	B	A	B	B	B	A	A	B	A	B
Bit Medido por Bob	0	0	1	0	1	0	0	1	1	0	0	1
Concordância de Bases	OK		OK	OK		OK		OK				OK
Seqüência Obtida	0		1	0		0		1				1
Bits anunciados para Correção de erros	0					0		1				
Chave Secreta			1	0								1

Figura 2: Exemplo de negociação de chave criptográfica utilizando o protocolo BB84

Uma série de análises da segurança do protocolo BB84 foi realizada nos últimos anos, apontando para sua a consistência. Uma análise detalhada dos ataques possíveis e um resumo das provas de segurança existentes é abordado em (Gottesman, D. e Hoi-Kwong, L., 2002). O protocolo tal como foi proposto é perfeitamente integrável no contexto das telecomunicações aeronáutica para a distribuição de chaves entre aeronaves e estações de solo, garantindo segurança incondicional para a comunicação entre os dispositivos. Devido à possibilidade de detecção de tentativa de invasão, o método ainda possibilita a ação de mudança de rota de comunicação e manutenção do tráfego de dados. Esse é um aspecto estritamente relevante para a alta disponibilidade exigida para o canal de dados no caso de veículos não-tripulados, os quais são extremamente sensíveis à falha na comunicação de dados. Em contrapartida, aspectos específicos e limitações da implementação da criptografia quântica em um ambiente aeronáutico, especialmente o fato da natureza móvel dos elementos da rede, devem ser considerados em um cenário realístico.

4. IMPLEMENTAÇÃO DE REDES UTILIZANDO CRIPTOGRAFIA QUÂNTICA E ANÁLISE DO CENÁRIO DE TELECOMUNICAÇÕES AERONÁUTICAS

A manipulação de fótons é bem conhecida e dominada atualmente, sendo que avanços recentes permitiram a construção de dispositivos capazes de manipular fótons individualmente. A reunião de LEDs modernos, a tecnologia atual de fabricação de fibras óticas de altíssima pureza e o domínio de transmissões aéreas utilizando lasers permitiu com que o protocolo de criptografia quântica fosse implementado com grande sucesso por diversos dispositivos. O grande entrave para o maior desenvolvimento da técnica consiste na impossibilidade de construção de amplificadores ou repetidores quânticos, área essa de extensa pesquisa. As distâncias alcançadas com fibras de alta qualidade, no entanto, já são suficientes para aplicações comerciais ou militares de segurança crítica, alcançando a ordem de centenas de quilômetros. A taxa de erros e a velocidade de transmissão vêm aumentando rapidamente com a participação de inúmeros laboratórios de pesquisa privada, tornando o custo de fabricação dos sistemas menor. Um conjunto de empresas já disponibiliza comercialmente equipamentos que realizam o protocolo BB84 sobre fibra ótica com eficiência suficiente para a integração com outros dispositivos de rede de sistemas comerciais, estabelecendo um link ponto-a-ponto.

A realização do protocolo BB84 em transmissões aéreas é alvo de intensa pesquisa internacional como forma de aumentar as distâncias máximas de comunicação e a possibilidade de cobertura de dispositivos móveis como aeronaves. A transmissão aérea se beneficia do grande coeficiente de transmissão do ar para freqüências de luz específicas, sendo a atmosfera fracamente dispersiva nesses casos e essencialmente isotrópica. O protocolo é realizado por meio de um feixe de laser pulsante que é colimado por telescópio simples emergindo com diâmetro de cerca de 10 a 30 cm. O receptor, tipicamente construído a partir de uma fotomultiplicadora ou diodo de foto-avalanche, possui um conjunto de filtros polarizadores que permite realizar medições sobre os fótons recebidos. Uma síntese do aparato necessário é mostrada na figura 3. Com a tecnologia atual é possível construir o conjunto do transmissor com massa de não mais que 3 kg, podendo ser embarcado em aeronaves e satélites (Riguidel, M., 2005). O receptor exige atenção especial, podendo ser construído atualmente com massa de 5 kg. O tratamento de alvos móveis é realizado com guias de onda por laser, possibilitando a localização do alvo com precisão suficiente para estabelecimento de comunicação.

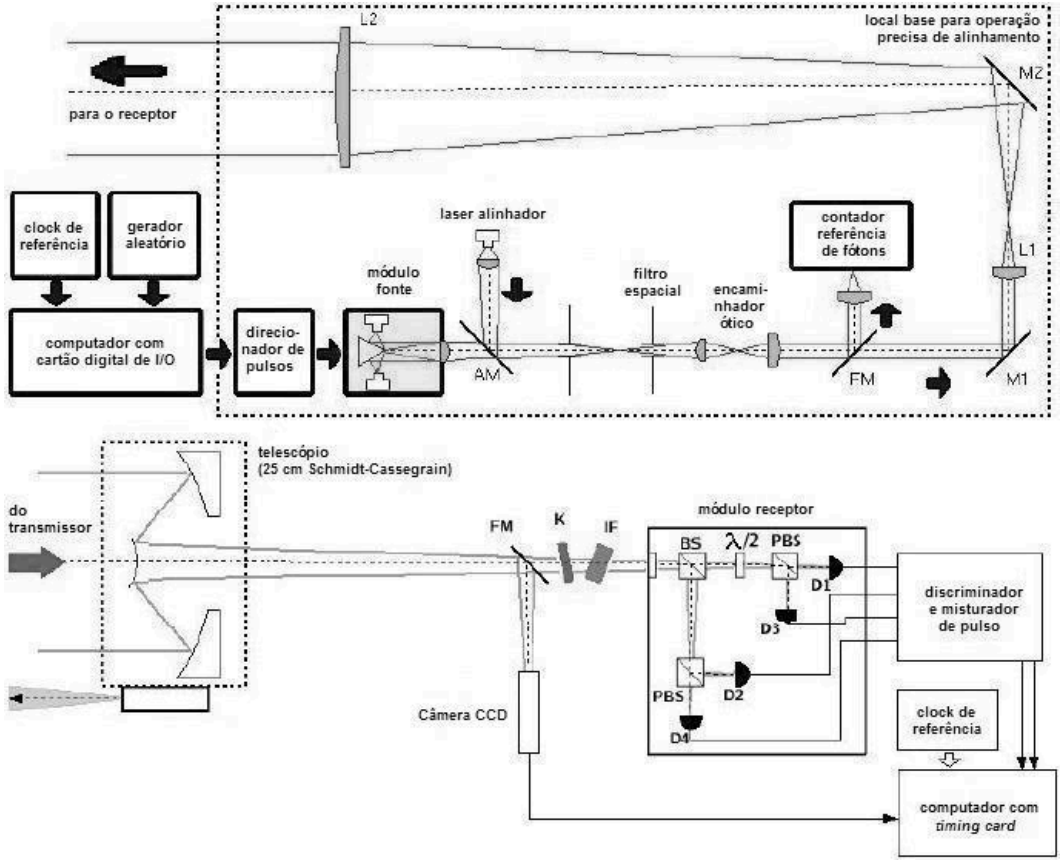


Figura 3: Resumo de aparato utilizado por um transmissor e receptor de sinal quântico

As principais realizações bem sucedidas de criptografia quântica pelo ar são representadas pelos experimentos:

- 1996 J. Franson, Baltimore : 150 m, diurno
- 1998 R. Hughes, Los Alamos : aprox. 1 km, noturno
- 2000 R. Hughes, Los Alamos : 1,6 km, diurno
- 2001 J. Rarity, QinetiQ : 1,9 km, diurno
- 2002 R. Hughes, Los Alamos : acima de 10 km
- 2003 P. Morris : 23,4 km, noturno

A mais recente realização de P. Morris demonstra teoricamente a viabilidade do estabelecimento de comunicação utilizando protocolo de criptografia quântica por distâncias acima de 1600 km (Kurtsiefer, C. *et al*., 2002). Esse resultado indica a viabilidade de um cenário em que utilizando satélites de baixa órbita, satélites de altitude média e satélites geoestacionários seja possível estabelecer uma rede completa de distribuição de chaves quânticas. A análise de viabilidade técnica da construção de uma rede global de distribuição de chaves quânticas utilizando a tecnologia de satélites atual foi demonstrada (Fedrizzi, A. *et al.*, 2005).

A possibilidade de estabelecimento de comunicação quântica entre satélites, dispositivos móveis e estações de solo permite considerar o método de criptografia quântica como uma solução viável para manutenção da segurança em redes aeronáuticas. Os principais desafios encontrados nesse cenário, provenientes principalmente da necessidade de alta disponibilidade dos dados pelas aeronaves em vôo, principalmente veículos aéreos não-tripulados, são:

- Grande sensibilidade dos equipamentos de recepção de sinal quântico a fenômenos metereológicos, especialmente nos 800 km inferiores da atmosfera, e a sensibilidade à iluminação de fundo. Esses pontos se tornam relevantes na operação de aeronaves em condições adversas e sobre regiões irradiadoras de luz como grandes cidades
- A existência de erros de transmissão limita a velocidade de geração da chave criptográfica , atualmente na ordem de 16000 bits/s para distâncias em torno de 2000 km e 6500 bits /s para distâncias em torno de 4000 km (Fedrizzi, A. *et al,.* 2005)

- Comunicação é feita ponto-a-ponto exigindo estabilidade de rastreamento, possibilidade de rotas múltiplas e equipamentos de sincronização e posicionamento sensíveis (Fedrizzi, A. *et al.,* 2005)
- Taxa de erros de comunicação na ordem de 2% a 7%

A evolução das técnicas de transmissão de chaves quânticas por espaços abertos provoca uma grande mudança de paradigma na comunicação entre veículos aéreos, especialmente os não-tripulados. A obtenção de uma rede completa e padronizada onde seja possível estabelecer comunicação incondicionalmente segura permitirá o estabelecimento de um canal de dados confiável, alcançando os níveis de segurança requisitados para a evolução do setor aeronáutico e permitindo que dispositivos não-tripulados possam assumir seguramente diversas funções críticas.

5. CONCLUSÃO

A crescente utilização da comunicação de dados em aeronaves e a maior utilização de veículos aéreos não-tripulados indicam a necessidade do atendimento de requisitos de segurança da informação para a operação segura, sendo que a fragilidade dos métodos de criptografia clássicos utilizados atualmente representa uma vulnerabilidade em curto prazo.

Neste trabalho foi mostrado que a utilização da técnica de criptografia quântica permitiria o atendimento dos requisitos de segurança para a rede de telecomunicações aeronáuticas necessário para manter um canal de dados confiável. A análise do protocolo quântico BB84 em um cenário realista de comunicação aérea mostrou que este é adequado e totalmente integrável à operação atual.

As técnicas de construção de dispositivos óticos apontam para a viabilidade de construção de uma rede quântica global para troca de chaves criptográficas utilizando a tecnologia de satélites corrente. A cobertura de alvos móveis foi demonstrada experimentalmente, possibilitando a distribuição de chaves para aeronaves em vôo.

A despeito das dificuldades encontradas na operação de distribuição de chaves quânticas em um ambiente aeronáutico, constatam-se claramente os benefícios que a utilização da criptografia quântica possibilita para a comunicação de dados entre aeronaves. Dessa forma, a pesquisa e desenvolvimento da técnica de criptografia quântica se mostram como fatores estratégicos para a operação de telecomunicação em redes aeronáuticas e para a evolução da tecnologia de veículos aéreos não-tripulados.

REFERÊNCIAS BIBLIOGRÁFICAS

Bennett, C. e Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing – *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, IEEE, Bangalore (India), v. 1, p. 175–179.

Elliott, C. (2002) Building The Quantum Networks – *Relatório Técnico,* BBN Technologies, USA.

Fedrizzi, A., Poppe, A., Loruenser, T., Maurhardt, O., Ursin, R., Boehm, H. R., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter H., Jennewein, T. e Zeilinger, A. (2005) Practical quantum key distribution with polarization entangled photons - *Optics Express*, v. 12, p. 3865-3866.

Gobby, C., Yuan, Z. L. e Shields, A. J. (2006) Quantum cryptography - *arXiv:quant-ph*, 3(207).

Gottesman, D. e Hoi-Kwong, L. (2002) Proof of Security of Quantum Key Distribution with Two-Way Classical Communications, *IEEE Transactions on Information Theory*, v. 49, p. 457.

ICAO (2002) *ATN Standards and Recommended Practices, 9705* (3ª ed.), International Civil Aviation Organization.

Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P. M., Tapster, P. R. e Rarity, J. G. (2002) A Step Towards Global Key Distribution – *Nature*, v. 419, p. 450.

Mayers, D. (2001) Unconditional Security in Quantum Cryptography - *JACM*, v. 48, no. 3, p. 351-406.

McMath, J. (2003) Aeronautical Telecommunications Network (ATN): Security, Key Management and Distribution - *AEEC Data Link Users Forum*, Titan Corporation, Hanscom, MA, USA.

Riguidel, M. (2005) Quantum Crypt – Enhancement of AGT Communications Security using Quantum Cryptography – *Relatório Técnico ENST/EEC/QC.12.01.WP3.A*, Eurocontrol e Telecom Paris, Paris, França.

Carlos Henrique Andrade Costa (carlos.costa@poli.usp.br)
João Batista Camargo Jr. (joao.camargo@poli.usp.br)
Grupo de Análise de Segurança, Escola Politécnica, Universidade de São Paulo
Av. Prof. Luciano Gualberto, travessa 3, n. 158, Cidade Universitária – São Paulo, SP, Brasil