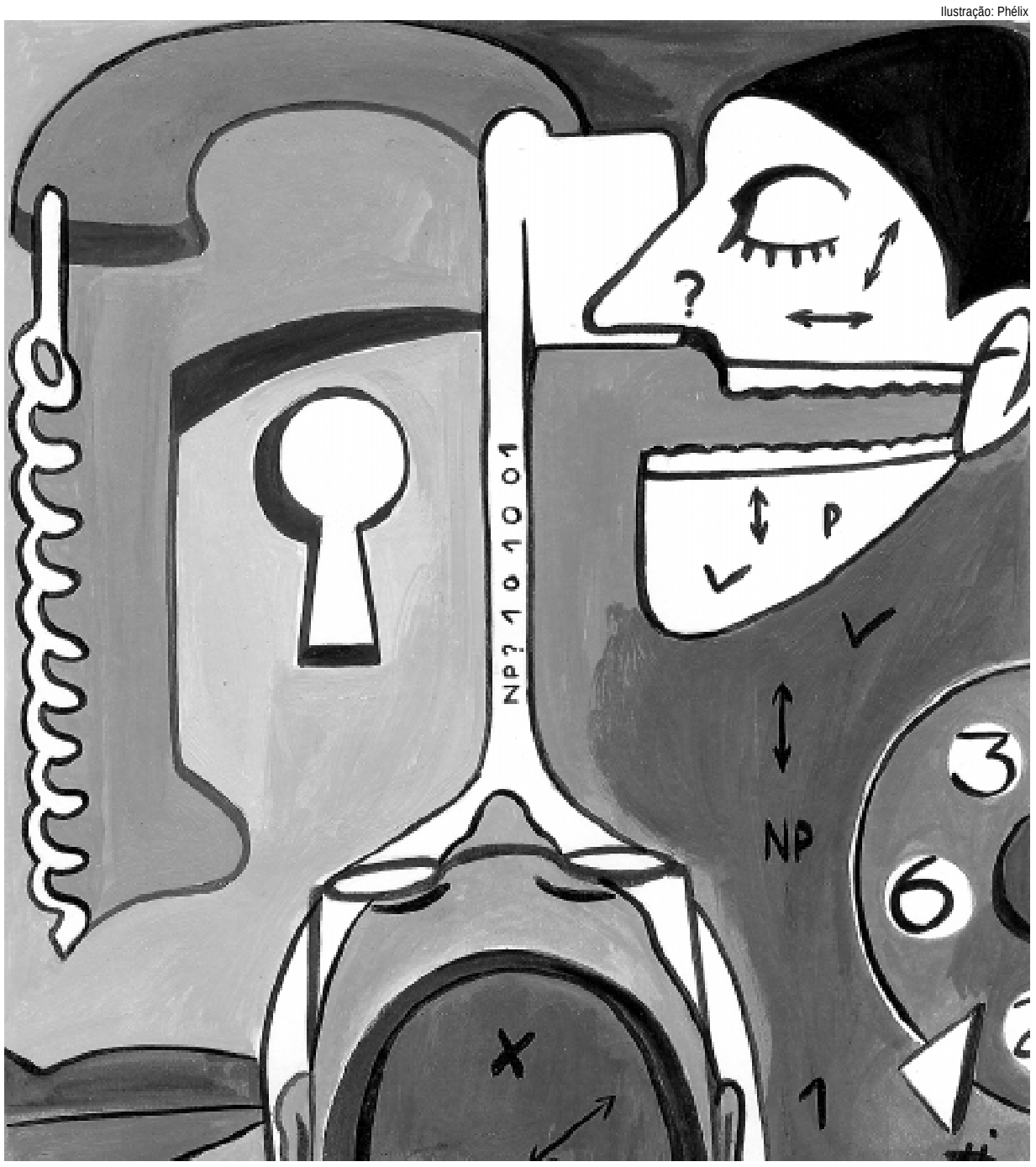
Professor do IFGW idealiza novo protocolo para distribuição de chaves da criptografia quântica

O que os cientistas reservam para Alice, Bob e a espiã Eva

LUIZ SUGIMOTO
sugimoto@reitoria.unicamp.br

Ilustração: Phélix



Vamos entrar no mundo de Alice, Bob e da espiã Eva, personagens conhecidíssimas da criptografia e que desassossegam a mente de pesquisadores absortos em desenvolver sistemas de transmissão de mensagens com total segurança, sejam pelo ar ou por fibras ópticas. A criptografia, ciência de transformar textos originais em informações ilegíveis, é tão antiga quanto a própria escrita. Houve o tempo em que Júlio César, imperador romano, enviava a cavalo mensagens cifradas, onde uma letra deveria ser substituída por outra que estava três posições à frente no alfabeto, na ingênua convicção de que, caso o mensageiro fosse capturado, o inimigo não conseguiria ler a ordem tática dada para vencer a batalha.

Sistema seria imune a falhas

A automação e principalmente o advento do computador dotaram a criptografia de complexos algoritmos matemáticos. Na Segunda Guerra, os ingleses conquistaram fama pela competência na quebra de códigos dos alemães: esta arma utilizada pelos aliados chama-se criptoanálise. Deve ter sido esse duelo na esfera da espionagem que inspirou os cientistas a adotarem os nomes de Alice e Bob, ao invés de símbolos matemáticos como "A" e "B" para identificar a origem e a recepção da mensagem, colocando Eva na escuta para avaliar os riscos de interceptação.

Vivendo agora numa época em que informação é sinônimo de poder, Alice e Bob se sofisticaram, e Eva também. Da privacidade do extrato bancário à encriptação das compras na Internet, tudo requer defesa contra prováveis interferências. O professor Antonio Vidiella Barranco, do Departamento de Eletrônica Quântica do Instituto de Física Gleb Wataghin (IFGW) da Unicamp, explica que a criptografia alcançou um refinamento que, na prática, impossibilita a quebra de uma mensagem, haja vista que os computadores atuais levariam anos para executar as operações matemáticas exigidas para decifrar um código. Na teoria, porém, já se aperfeiçoam os computadores quânticos, que seriam capazes de realizar tais operações em segundos, para delírio de Eva. Por isso, físicos, engenheiros, matemáticos, cientistas da computação correm atrás de uma nova chave de segurança.

Contra o risco oferecido por tamanho poder computacional, elabora-se a criptografia quântica, que seria imune a falhas de segurança. Antonio Vidiella, um dos poucos pesquisadores que se ocupam do tema no país, acredita ter idealizado um novo protocolo envolvendo feixes de laser que apresenta inúmeras vantagens em relação a outros estudados no mundo. E tem pressa em finalizar um artigo para publicação, antes que Eva nos ouça. "O trabalho foi apresentado apenas no 27º Encontro de Física de Matéria Condensada em Poços de Caldas, no início de maio. Trata-se de uma proposta concreta, que ainda precisa ser aprimorada e testada em laboratório quanto à questão da segurança, mas que pode perfeitamente ser desenvolvida no Brasil. Nosso objetivo é gerar um protocolo para ser efetivamente usado, como na transmissão de dados governamentais ou em qualquer operação que exija sigilo", adianta o pesquisador.

Foto: Neldo Cantanti

O professor Antonio Vidiella Barranco, do IFGW: atrás de uma nova chave de segurança

Historinha – Para tornar compreensível a nova proposta, Vidiella repassa ao menos o básico da criptografia recente. Explica que, já no começo do século 20, chegou-se a uma forma de transmitir uma mensagem de maneira indecifrável, a partir do código binário, basicamente uma seqüência aleatória de zeros e uns, que seria a chave. "Alice faz uma operação envolvendo sua mensagem com esta seqüência aleatória, formando a mensagem cifrada que é transmitida a Bob. Ficou provado que havendo uma seqüência de números com o mesmo tamanho da mensagem, é impossível decifrá-la, desde que não se conheça a chave", afirma o professor do IFGW. No entanto, como Alice faz a chave chegar até Bob para que ele decifre a mensagem?. "A distribuição da chave entre as partes interessadas foi o problema surgido", observa.

Alice e Bob, no caso, teriam que se encontrar para compartilhar a chave, correndo o risco de interceptação. Se Alice optasse por um mensageiro, ele bem que poderia ser subornado por Eva. Um site da Associação de Professores de Matemática traz uma historinha ilustrativa em que Alice e Bob vivem isolados e só podem se comunicar pelo correio. Mas sabem que o carteiro lê todas as cartas. Alice pensa em enviar a carta dentro de um cofre, fechado a cadeado. Mas como fazer a chave chegar a Bob para que ele abra o cofre? Simples: Bob recebe o cofre e fecha-o com um segundo cadeado, do qual possui a chave. Remete o cofre com os dois cadeados pelo correio. Alice remove um cadeado com sua chave e devolve o cofre. Bob só tem que utilizar sua chave para abrir seu cadeado, enquanto o carteiro fica a ver navios.

Chave pública – Esta historinha inspirou a criação do sistema RSA, por três jovens americanos, Whitefield Diffie, Martin Hellman e Ralph Merkle, e hoje largamente utilizado. Segundo a idéia, para que Bob possa receber uma mensagem, ele primeiramente escolhe uma chave secreta, a partir da qual constrói uma chave pública. Alice utiliza essa chave pública para criptografar a mensagem e enviá-la a Bob, que por sua vez decifra a mensagem usando a sua chave privada. Eva, mesmo tendo interceptado os números públicos, ficará a ver navios. As chaves não são trocadas, mas tanto Alice como Bob acabam por poder abrir o cofre, sem que Eva o consiga.

Temos então o sistema de chaves públicas, que serve aos bancos, Internet e a tantos outros serviços. "Colocando-se alguns teoremas por trás desta lógica, chegamos a combinações de números primos que nenhum computador, hoje, é capaz de fatorar rapidamente. Esta criptografia é muito conveniente, porque posso mandar mensagens para várias pessoas", observa Vidiella. Mesmo esta criptografia, porém, apresenta uma fragilidade potencial, que é a incerteza quanto à sua segurança. Segundo o pesquisador, os computadores quânticos em gestação teriam uma capacidade de paralelismo muito alta, conseguindo fatorar números enormes em fatores primos com uma velocidade de poucos segundos. É na busca de uma alternativa que se encaixa seu trabalho.

Protocolo BB84 – "Faz vinte anos que os físicos Bennett e Brassard propuseram uma nova forma de criptografia, a quântica. Este protocolo foi denominado BB84. Nele, a segurança é baseada nas leis da natureza, em limitações naturais. Os valores de grandezas físicas nem sempre podem ser acessados com precisão absoluta. Isso fica patente na mecânica quântica, onde desde o início ficou óbvio que o acesso a informações de sistemas microscópicos, em geral, era limitado. A idéia é aplicar essas idéias para transmitir informação segura. Na verdade, a criptografia quântica é uma maneira de distribuir chaves", explica Vidiella.

Para esta distribuição se utilizariam as propriedades quânticas da luz. Alice gera luz com determinadas características, transmitindo-a para Bob, que realiza certas medidas. Alice sabe os parâmetros para codificar a informação da chave que usou e Bob anota o que mediu. Alice e Bob estabelecem então uma comunicação adicional, através de um canal público, descartando uma série de bits e destilando a chave que será compartilhada. Como Eva pode estar interceptando a transmissão de luz, isso causará uma interferência que será certamente percebida por Bob. "Ocorre que o novo protocolo exige uma fonte de luz muito especial, uma fonte de único fóton, gerada por um átomo estimulado ou pontos quânticos. Já se chegou perto dela, mas há a necessidade de obter uma luz controlada, em que se consiga gerar um fóton de cada vez, o que não é fácil de se fazer", afirma.

Idéia simples – Outro problema é como propagar essa luz, seja pelo ar ou por fibra óptica. Grupos da Suíça, que utilizaram laser atenuado, conseguiram transmitir esta chave quântica num raio de 100km através de fibra óptica. Pelo ar é mais complicado, mas já existem transmissões de até 10km. "Percebi que seria interessante fugir das propostas pesquisadas no exterior, a exemplo do laser atenuado, e buscar outros protocolos que se adaptassem à fonte de luz laser que já dominamos e que é mais fácil de gerar e controlar", recorda o professor, que decidiu mergulhar no tema juntamente com o doutorando Luiz F. M. Borelli.

A idéia, que surgiu de maneira surpreendentemente natural diante de tanto esforço despendido pela comunidade científica, é fazer uso da polarização do laser, pois a direção do campo elétrico é perfeitamente controlável. "Posso mandar um feixe na horizontal, vertical, como eu quiser. O receptor pode medir facilmente esta polarização, onde estaria codificada a chave. Além disso, a taxa de transmissão de dados usando fontes de um único fóton é baixa. É como mandar um bit e depois o outro, uma limitação em se tratando de grandes volumes de informações. Com o laser a taxa é bem maior", justifica o pesquisador. Antonio Vidiella espera concluir o trabalho teórico em um mês, com a ressalva de que a questão da segurança é mais delicada. "Todo protocolo é passível de ataques. É uma proposta embrionária, com ótimas perspectivas, mas precisamos confirmar, tanto teórica como experimentalmente, que a segurança vai ser boa o suficiente", finaliza.