# Aplicação de Algoritmo Genético para Determinação de Chaves Usadas em Criptografia Óptica Mediante Fatiamento Espectral

Felipe Luiz Tortella, Carlos Miguel Tobar Toledo e Marcelo Luís Francisco Abbade

***Resumo*— A necessidade de aprimorar a segurança de informação está estimulando a adoção de técnicas de criptografia na camada física das redes de telecomunicações. Uma das técnicas recentemente investigadas para este propósito, no escopo de redes ópticas, consiste em dividir um dado sinal em diversas fatias espectrais e em distorcer o conteúdo de cada fatia para codificar o sinal original. O conjunto de parâmetros de distorção constitui uma chave de criptografia. Neste trabalho, investiga-se a utilização de um algoritmo genético (AG) para gerar chaves desse tipo. Considera-se que as chaves são aceitáveis apenas quando as taxas de erro de bit (*bit error rate*, BER) do sinal codificado é suficientemente alta e quando a BER do sinal decodificado é consideravelmente baixa. Os resultados de simulações numéricas indicam que o AG produziu chaves válidas em mais de 95% das vezes, nos melhores casos, quando as BERs mencionadas anteriormente são de $2\cdot10^{-1}$ e $10^{-15}$ respectivamente.**

***Palavras-Chave*— *Segurança e criptografia óptica; Algoritmo genético; Comunicações ópticas.***

***Abstract*—Necessity of enhancing information security is stimulating the adoption of new cryptographic techniques at the physical layer of telecommunication networks. In the scope of optical networks, one of these recently investigated techniques consists on splitting a signal in several spectral slices and on imposing distortions to each of these slices to encode the original signal. The set of distortion parameters constitutes a cryptographic key. In this work, is investigated the use of a genetic algorithm (GA) to generate keys of this type. In particular, only those keys that provide an encoded signal with a sufficiently high bit error rate (BER) and a decoded signal with a satisfactorily low BER are acceptable. Numerical best simulation results indicate the GA generated acceptable cryptographic keys in more than 95% of the considered potential keys, in the cases where the above BERs are respectively of $2\cdot10^{-1}$ and $10^{-15}$.**

***Keywords*— *Optical security and encryption; Genetic algorithm; Optical communications.***

## I. INTRODUÇÃO

Segundo um estudo realizado com 350 empresas de 11 países [1], 47% das brechas de segurança em redes corporativas são decorrentes de ataques criminosos ou maliciosos. Essa mesma referência ainda indica que o custo médio de cada brecha de segurança foi, em 2015, de US$ 3,79 milhões. Observa-se que, além do mundo corporativo, ataques do tipo podem comprometer criticamente os setores governamental e de defesa. Nesses casos, além de danos financeiros diretos, a perda de sigilo pode prejudicar a implantação de temas estratégicos. Em todos esses casos, ainda há degradação da imagem e da credibilidade das instituições envolvidas. Por todas essas razões, torna-se premente a adoção de novas formas de criptografia e de codificação de dados em redes de telecomunicações.

As redes ópticas operam sobre um meio confinado e são, portanto, inerentemente mais seguras que as redes sem-fio. Além disso, o confinamento do campo eletromagnético no interior das fibras e a necessidade de utilização de equipamentos mais complexos, que os usados em redes de sinais eletrônicos, também fazem com que as redes ópticas sejam mais confiáveis que as outras redes cabeadas. Mesmo assim, é possível utilizar divisores ópticos e acopladores de grampo (*clip-on couplers*) [2] para desviar sinais ópticos para rotas não autorizadas. A baixa perda causada pela inserção desses equipamentos dificulta a identificação de sua utilização e constitui motivo de preocupação para as operadoras de telecomunicações. Uma estratégia considerada para minimizar a chance de sucesso de furto de sinais por desvio de rota é criptografar esses sinais na própria camada física.

A distribuição de chaves quânticas (*quantum key distribution*, QKD) constitui o método mais seguro para criptografia na camada física [3]. No entanto, a utilização prática desta ainda está atualmente restrita a distâncias de poucas centenas de quilômetros e a taxas de poucas centenas de Mbits/s [4]. Outra técnica que está sendo considerada no contexto de redes ópticas é a criptografia baseada em caos [5]. Contudo, apesar de conceitualmente promissora, o mecanismo de sincronização entre o receptor e o transmissor requerido por essa abordagem ainda não pode ser atendido em redes comerciais. Outros esquemas baseiam-se na implementação de codificação espectral de fase (*spectral phase encoding*, SPE) [6], codificação espectral de amplitude (*spectral amplitude encoding*, SAE) [7] e codificação espectral de atraso (*spectral delay encoding*, SDE) [7-10]. Essas três estratégias são interessantes por serem aplicadas a canais compatíveis com a tecnologia de multiplexação por divisão em comprimento de onda (*wavelength division multiplexing*, WDM) e, portanto, em princípio, podem ser usadas em redes comerciais.

Em particular, [8-10] abordam a aplicação simultânea de SPE e SDE, que aumenta expressivamente a robustez da codificação considerada. No entanto, a utilização prática dessa técnica de dupla codificação, chamada de codificação espectral de fase e atraso (*spectral phase and delay encoding*, SPDE), requer que as chaves criptográficas sejam dinamicamente alteradas, para minimizar as chances de sucesso de ataques

Felipe Luiz Tortella e Carlos Miguel Tobar Toledo: Pontifícia Universidade Católica de Campinas, Campinas-SP, Brasil. Marcelo Luís Francisco Abbade: UNESP- Univ Estadual Paulista, São João da Boa Vista-SP, Brasil, E-mails: felipetortella@gmail.com, tobar@puc-campinas.edu.br, marcelo.abbade@sjbv.unesp.br. Este trabalho foi financiado pelo CNPq (574017/2008-9, 311137/2014-8) e pela FAPESP (08/57857-2).

maliciosos. Conforme a descrição da Seção II, essas chaves são determinadas a partir de parâmetros de fase e de atraso escolhidos para distorcer os sinais que serão criptografados. No entanto, uma chave só é válida se, entre outras características, garantir que a taxa de erro de bit (*bit error rate*, BER) do sinal codificado seja suficientemente alta e que, simultaneamente, a BER do sinal decodificado seja consideravelmente baixa. Sendo assim, nem todas as chaves criptográficas possíveis são aceitáveis.

Neste trabalho, investigou-se a aplicação de um algoritmo genético (AG) para definir chaves criptográficas que sejam aceitáveis para a SPDE. A validade dos resultados do AG foi verificada por meio de simulações computacionais realizadas no *software* VPITransmissionMaker™ 9.5. No melhor de nosso conhecimento, essa é a primeira vez que uma análise do tipo é apresentada na literatura.

O restante do trabalho está organizado da seguinte maneira. A Seção II apresenta uma breve revisão sobre a SPDE. O AG utilizado e o cenário de simulação considerado estão descritos, respectivamente, nas Seções III e IV. Os resultados obtidos são apresentados na Seção V. Por fim, as conclusões são abordadas na Seção VI.

## II. Codificação Espectral por Fase e Atraso

Na SPDE, um sinal óptico de banda $B$ é dividido em $n$ fatias espectrais, como ilustrado no diagrama de blocos do codificador da Fig. 1. A seguir, os sinais da $i$-ésima ($i$= 1, ..., $n$) fatia espectral são submetidos a um desvio de fase $\phi_i$ e a um atraso $\tau_i$, cujos valores máximos são, respectivamente, $\phi_{max}$ e $\tau_{max}$. Fisicamente, cada componente espectral, situado em uma frequência $f$ e submetido a um atraso $\tau_i$, sofre um desvio de fase de $-2\pi f\tau_i$. Portanto, atrasos constantes implicam em variação linear da fase ao longo da banda $B/n$ de cada fatia espectral. Após isso, os sinais de cada fatia são multiplexados e geram uma versão criptografada do sinal de entrada que é transmitida por uma rede óptica transparente (*transparent optical network*, TON) até um receptor autorizado.

Para recuperar o sinal original, esse receptor utiliza um decodificador que é fisicamente idêntico ao codificador, mas que submete os sinais da $i$-ésima fatia espectral a desvios de fase e a atrasos complementares aos usados na codificação, respectivamente, por $\phi_{max} - \phi_i$ e $\tau_{max} - \tau_i$. A utilização desses valores retira as distorções introduzidas pelo codificador e faz com que o sinal na saída do multiplexador do decodificador seja, idealmente, idêntico ao sinal na entrada do codificador. Na prática, o perfil não ideal, dos filtros do codificador e do decodificador, fará com que o sinal decodificado difira do sinal introduzido na entrada do decodificador. A descrição matemática desses sinais é apresentada em [8]. Além disso, os impedimentos físicos impostos durante a transmissão do sinal pela TON também contribuirão para diferenças entre os sinais decodificado e de entrada.

Observa-se que os atrasos escolhidos são da ordem de períodos de símbolo, $T_s$. Assim, a codificação espectral por atraso faz a forma do sinal codificado depender da própria informação que é, pressupostamente, desconhecida pelos intrusos. Essa característica aumenta a robustez da criptografia considerada e constitui uma das principais vantagens da SDE e da SPDE sobre a SPE [7, 8].

Durante a propagação pela TON, o sinal criptografado pode ter parte de sua potência desviada para uma rota não autorizada e ser interceptado por algum intruso. Os espiões, em princípio, não conseguirão compreender o significado do sinal criptografado. No entanto, esses intrusos podem realizar ataques e/ou monitorar as formas de onda do sinal recebido [7], para extrair informações que permitam decodificá-lo. Para minimizar o sucesso dessas abordagens, é interessante que as chaves criptográficas sejam substituídas ao longo do tempo.

Nota-se que essas chaves correspondem aos parâmetros de distorção utilizados em cada fatia $\phi_i$ e $\tau_i$ ($i$= 1, ..., $n$). Neste trabalho, designa-se a chave criptográfica $K$ por $K$= {$\phi_1$, $\tau_1$; $\phi_2$, $\tau_2$; ...; $\phi_n$, $\tau_n$}. As fases $\phi_i$ podem assumir quaisquer valores no intervalo de 0 a 360º e $\tau_i$ podem, em princípio, variar desde frações de até centenas de períodos de símbolo. A possibilidade de variação contínua de $\phi_i$ e $\tau_i$ implica em um número infinito de chaves potenciais. No entanto, nem todas essas chaves podem ser usadas. De fato, chaves válidas requerem, minimamente, que: i) a BER do sinal codificado seja maior que um determinado valor crítico, $BER_c$, ii) a BER do sinal decodificado seja menor que um outro valor crítico, $BER_d$. O requisito (i) é necessário para que o sinal codificado tenha uma BER superior àquela que pode ser corrigida pelo mecanismo de correção antecipada de erro (*forward error correction*, FEC), $BER_{FEC}$, empregado na transmissão do sinal. Neste trabalho, considera-se que a FEC pode corrigir sinais com BER de até $BER_{FEC}= 2\cdot10^{-3}$ e que $BER_c$ é 10 vezes maior, $BER_c= 2\cdot10^{-2}$. O requisito de (ii) é óbvio e deve ser garantido mesmo após a propagação do sinal pela TON. Neste trabalho, adotou-se $BER_d< 1\cdot10^{-15}$ para o caso de uma transmissão *back-to-back* (codificador ligado diretamente no receptor). Observa-se que essas restrições são inerentes e obrigatórias para qualquer técnica de criptografia na camada física.

## III. Algoritmo Genético

Um AG corresponde a uma busca baseada no mecanismo de seleção genética natural, a partir de uma técnica de otimização estocástica [11]. Assim, inicialmente obtém-se, por sorteio, uma população de indivíduos, as potenciais soluções, que são submetidos a três operações evolutivas: o cruzamento (*crossover*), por meio do qual dois indivíduos originam um ou

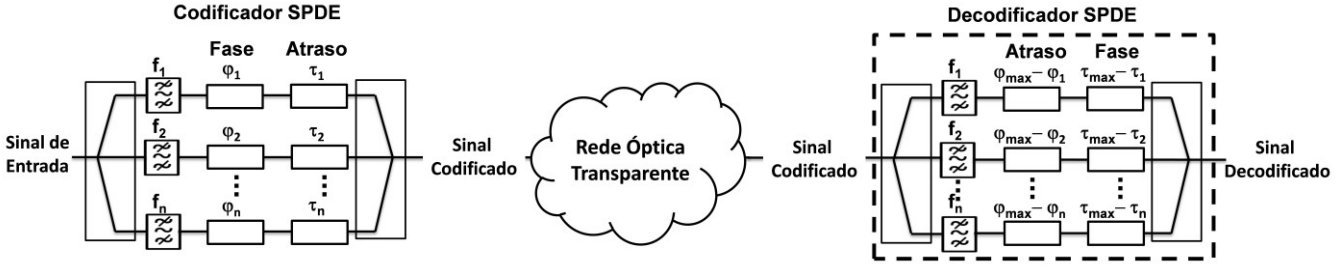


Fig. 1. Diagrama de blocos para a codificação espectral por fase e atraso.

mais outros potenciais indivíduos com a combinação de suas características (ou genes); a mutação, através da qual um determinado indivíduo tem uma ou mais de suas características alteradas e, se a evolução natural for considerada, esse indivíduo seria um daqueles frutos do cruzamento; e seleção, a partir da qual mede-se a aptidão dos indivíduos existentes e produzidos nos cruzamentos e nas mutações, e mantêm-se aqueles mais aptos. Ao final de um ciclo de cruzamentos, mutações e seleção, define-se uma nova geração de indivíduos.

Com essa ideia geral, foi implementado um AG que busca potenciais chaves que possam ser usadas para a SPDE. A ferramenta permite que vários aspectos do AG sejam configurados: o número de fatias espectrais, ou seja, o número de genes da chave potencial, cada qual constituído de um desvio de fase e um atraso; o tamanho da população, que, se for a inicial, seus indivíduos são definidos por sorteio; as condições de parada, que correspondem a um número máximo de gerações ou que impliquem que uma chave potencial atinja um patamar mínimo de aptidão; uma taxa de cruzamentos, $C$, ou seja, um valor que determina quantos indivíduos potenciais devem ser gerados por cruzamento; uma taxa de mutação, $M$, ou seja, um valor que determina quantos potenciais indivíduos sofrerão mutação; o tipo de cruzamento, que varia entre circular, um ponto de cruzamento ou dois pontos de cruzamento; e o tipo de seleção, definido entre roleta, truncamento e elitismo. Neste trabalho, os indivíduos correspondem a chaves e ambos estes termos serão utilizados de maneira intercambiável no restante do texto.

A operação de cruzamento considera $C$ para gerar, a partir da geração atual uma quantidade de novos e potenciais indivíduos. A primeira geração terá um número de indivíduos definidos por sorteio, cuja aptidão é verificada, ou seja, há observância dos requisitos (i) e (ii) discutidos anteriormente. Para essa verificação usa-se o VPITransmissionMaker™ 9.5 (Fig. 2). A partir dessa "Geração 0", sorteiam-se pares de indivíduos que não se repetem, para, em cada cruzamento, obter um potencial novo indivíduo.

Um cruzamento considerando um ponto ocasiona a divisão de cada um de dois indivíduos em duas sequências de pares $\phi_i$ e $\tau_i$ : ($\phi_1$ ,$\tau_1$) a ($\phi_k$ ,$\tau_k$) e ($\phi_{k+1}$ ,$\tau_{k+1}$) a ($\phi_n$ ,$\tau_n$), sendo $k \leq n$-1 um número inteiro sorteado. Dois filhos são definidos juntando-se a primeira sequência do primeiro indivíduo com a segunda sequência do segundo indivíduo e juntando-se a primeira do segundo com a segunda do primeiro.

Com dois pontos de cruzamento, obtém-se três sequências de pares $\phi_i$ e $\tau_i$, com a troca da segunda sequência (do meio) dos indivíduos, para gerar dois potenciais novos indivíduos. A posição dos dois pontos é sorteada.

No cruzamento circular, todos os pares $\phi_i$ e $\tau_i$, do segundo indivíduo são colocados após os do primeiro indivíduo, e os pares deste primeiro após os do segundo, formando um círculo de pares que será cortado em duas sequências de pares de tamanho $n$. O local de corte é decidido por sorteio.

A taxa de mutação determina quantos potenciais indivíduos terão um dos seus genes alterado. É sorteado um $\phi_i$ ou um $\tau_i$ de um potencial indivíduo, também sorteado. O $\phi_i$ ou $\tau_i$ terá invertido um bit sorteado da representação binária de seu valor.

Os potenciais novos indivíduos passarão necessariamente pela avaliação de aptidão no VPITransmissionMaker™ 9.5. Seleciona-se, então, uma quantidade de indivíduos equivalente ao tamanho da nova geração. Na seleção por roleta, os indivíduos mais aptos recebem uma probabilidade maior do que a dos menos aptos, para constarem na próxima geração. Neste tipo de seleção, indivíduos pouco aptos têm chance de estar na nova geração. Na seleção por truncamento, os mais aptos passam para a nova geração, enquanto na seleção por elitismo, faz-se uma seleção por roleta, mas apenas dos indivíduos mais aptos.

## IV. Descrição das Simulações

As simulações realizadas são relativas a um sinal óptico de 200 Gbps modulado em uma portadora de 193,1 THz por modulação de amplitude em quadratura (*quadrature amplitude modulation*, QAM) de 16 símbolos, 16-QAM. Antes de ser modulado, o sinal é passado por um filtro de Nyquist com um fator de decaimento (*roll-off*) de 0,1, propiciando que o sinal óptico tenha uma banda $B \approx$ 55 GHz. O codificador é conectado diretamente ao decodificador (configuração *back-to-back*) e a codificação é feita em sete fatias espectrais. Embora não existam restrições da SPDE neste sentido, a escolha de $\tau_i$ foi restrita a valores múltiplos de $T_s$, no intervalo $0 \leq \tau_i \leq 10\ T_s$, e $\phi_i$ foi selecionada no intervalo de 0 a 180º, em passos de 1º. Além disso, como este foi o primeiro trabalho sobre o assunto, optou-se por avaliar o caso mais simples correspondente a fatias espectrais geradas por filtros de perfil retangular.

A Fig. 2 apresenta um diagrama de blocos relativo às simulações realizadas. É feita uma cossimulação entre o programa desenvolvido por nossa equipe para integrar o AG e o *software* VPITransmissionMaker™ 9.5. Em um dado instante, o AG gera certa chave criptográfica potencial $K_j = \{\phi_{1j}, \tau_{1j}; \phi_{2j}, \tau_{2j}; ...; \phi_{7j}, \tau_{7j}\}$. Os parâmetros dessa chave são passados para o *software* VPITransmissionMaker™ 9.5 que simula a codificação e a decodificação do referido sinal QAM de 200 Gbps pela chave $K_j$. Esse *software* também avalia os valores de $BER_c$ e $BER_d$ e os informa ao AG. Caso seja considerada válida a chave, $BER_c > 2 \cdot 10^{-2}$ e $BER_d < 1 \cdot 10^{-15}$, $K_j$ é considerada apta e poderá vir a ser utilizada para a geração de novas chaves potenciais pelo AG, se sua aptidão estiver entre as melhores, de acordo com a descrição da Seção III. Por outro lado, se não for considerada válida, $K_j$ é descartada.

Nas simulações realizadas, o AG foi configurado para operar com cruzamento circular com taxas de 25%, 50% e 75%, combinadas com taxas de mutação de 4% e 5%, e seleção por elitismo. Em cada uma das nove execuções de cada combinação, inicialmente, foram gerados 100 indivíduos (chaves válidas) para a Geração 0. A partir desses indivíduos-

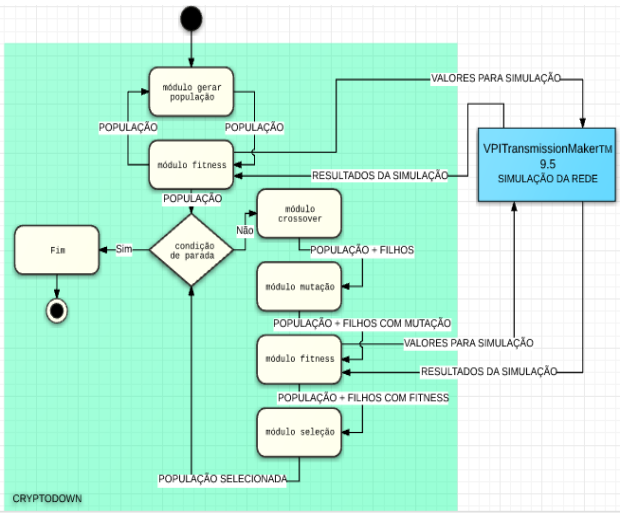


Fig. 2. Diagrama de blocos para a cossimulação entre o *software* que implanta o AG e o VPITransmissionMaker™ 9.5.

pais, o AG foi executado durante 20 gerações para gerar indivíduos com sua aptidão validada, frutos dos cruzamentos e das mutações. Considerando pais e filhos, ao final da primeira iteração, foram sorteados 100 indivíduos aptos, que foram submetidos ao AG para gerar novos indivíduos válidos para a segunda geração e, assim, sucessivamente. Desse modo, o AG foi executado para gerar novos indivíduos válidos na *i*-ésima geração, a partir de 100 mais 26, 50 ou 76 (da (*i-1*)-ésima geração de) indivíduos válidos, por conta da taxa de cruzamentos de 25, 50 e 75%, segundo as taxas de mutação. Os indivíduos não-aptos e menos aptos foram descartados porque os resultados indicaram que este procedimento aumentava a porcentagem de chaves válidas nas gerações posteriores.

Neste trabalho, o AG teve alterada a sua condição de parada. Uma execução com cossimulação é interrompida quando: a) o AG não consegue gerar 26, 50 ou 76 indivíduos válidos em uma dada geração ou b) quando o AG gera 26, 50 ou 76 indivíduos válidos em cada uma de 20 gerações consecutivas. Assim, caso (b) ocorra, a execução com cossimulação terá gerado 520, 1000 ou 1520 chaves válidas, durante suas 20 gerações.

## V. Resultados

Em todos os casos simulados neste trabalho, o AG foi capaz de encontrar todas as chaves esperadas para a geração em questão. Isto é, apenas a condição de parada (b) foi utilizada. A Fig. 3 mostra gráficos sobre a evolução do percentual de chaves válidas, PCV, em 20 gerações de nove execuções. Os gráficos referem-se a taxas de cruzamento de *C*= (a) 25%, (b) 50% e (c) 75%. Assim, como mencionado anteriormente, o número de chaves válidas após as 20 gerações para cada um desses valores de C é de, respectivamente, 520, 1000 e 1520. A Fig. 3 também compara o PCV para taxas de mutação *M*= 4 e 5%. Nos piores casos, na média de (C= 75%; M=4%) e de (C= 75%; M=5%), o AG geraram, em média, entre ~91,1% e ~91,7% de chaves válidas. Nos melhores casos, em várias execuções, houve 100% de chaves válidas. O número total de chaves geradas, em cada uma das nove execuções por combinação, foi de 3040 = (520+1000+1520).

A Fig. 4 mostra estatísticas referentes aos dados da Fig. 3. A média e a mediana do PCV de todas as 54 execuções são praticamente constantes para os três valores de *C* considerados. Isso sugere que o número de chaves considerado (entre 520 e 1520) é suficientemente grande para gerar boas estatísticas do AG aplicado. Observa-se, também, que a média e a mediana são praticamente as mesmas para as taxas de mutação de 4 e de 5%. Nota-se ainda (eixo da direita) que o desvio padrão do PCV oscila entre 2,1 e 7,7%. Isso é consequência de o desempenho do AG, observado na Fig. 3, ser aproximadamente o mesmo para todas as gerações de todas as execuções, na

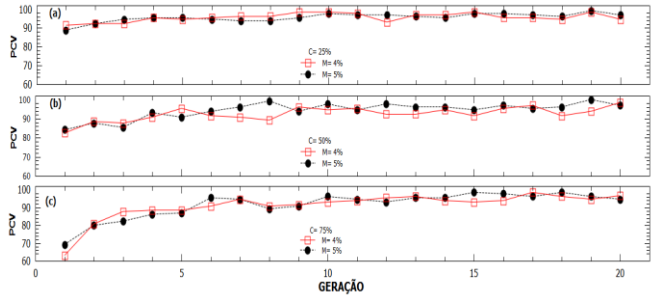


Fig. 3. Percentual de chaves válidas (PCV) para diferentes taxas de *crossover*, *C*, e de Mutação, *M*.

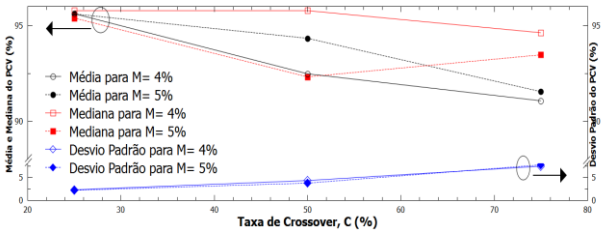


Fig. 4. Percentual de chaves válidas (PCV) para diferentes taxas de *crossover*, *C*, e de Mutação, *M*.

média.

A título de exemplo, a Tabela I mostra as 10 chaves mais aptas, com menor $BER_d$, entre aquelas encontradas pelo AG para C= 50% e M= 5%. Essa tabela mostra que os parâmetros das chaves válidas são bem distintos entre si. Pode, no entanto, ocorrer de duas ou mais dessas chaves terem genes similares. Assim, a estratégia que determinará qual chave substituirá outra deve garantir certo grau de dissimilaridade entre chaves sucessivas, em termos de troca, para reduzir as chances de decodificação de sinais por intrusos.

A terceira coluna da Tabela I mostra o valor da BER do sinal codificado para 10 chaves consideradas. Observa-se que o maior valor obtido é 0,201, que está ~10 vezes acima do limite considerado de $2{\cdot}10^{-2}$. O menor valor de $BER_c$ para estes dados é de 0,108. Os valores da BER do sinal decodificado não estão indicados na Tabela I porque são todos menores que $10^{-15}$ e, abaixo desse valor a precisão do VPITransmissionMaker™ 9.5 é limitada. No entanto, observa-se que os valores de $BER_c$ indicados por esse *software*, várias ordens de grandeza abaixo de $10^{-15}$, são similares àqueles obtidos nas configurações *back-to-back* relatadas em [8], suficientes para permitir a propagação dos sinais em questão por distâncias de até 400 km. A Fig. 5 mostra os espectros e os diagramas de constelação para uma chave que atenda os critérios de BER requeridos (como qualquer chave da Tabela I) para (a) o sinal QAM de entrada, (b) o sinal codificado e (c) o sinal decodificado. A constelação do sinal codificado está bastante difusa em relação à do sinal de entrada. Esse resultado é desejado e é consequência direta de ter sido escolhido um valor alto de $BER_c$. A constelação do sinal decodificado apresenta símbolos bem definidos, mas mais dispersos que aqueles relativos ao sinal de entrada. Isso pode ser explicado, ao menos parcialmente, pela limitação em banda

TABELA I. Exemplos de Chaves Válidas e Taxas de Erro de Bits Relacionadas

| **Geração** | **Chave Criptográfica** $K= \{\phi_1, \tau_1/T_s; \phi_2, \tau_2/T_s; ...; \phi_7, \tau_7/T_s\}$[a] | $\boldsymbol{BER_c}$ |
|---|---|---|
| 12 | $K_1$={123,1;116,7;104,10;29,9;113,7;170,4;106,4} | 0,197 |
| 19 | $K_2$={3,1;92,4;154,1;75,2;123,1;116,7;104,10} | 0,201 |
| 18 | $K_3$={126,7;126,7;167,7;94,8;6,7;167,1;172,4} | 0,131 |
| 16 | $K_4$={68,3;154,1;144,7;105,6;2,1;92,4;135,1} | 0,192 |
| 6 | $K_5$={5,9;69,8;125,6;97,9;37,7;89,3;56,6} | 0,190 |
| 5 | $K_6$={68,3;154,1;144,7;105,6;2,1;92,4;154,1} | 0,192 |
| 14 | $K_7$={98,4;154,1;92,3;113,3;170,4;106,4;126,7} | 0,191 |
| 6 | $K_8$={84,1;29,9;113,7;170,4;106,4;126,7;95,2} | 0,199 |
| 6 | $K_9$={74,4;167,7;91,1;8,9;177,6;37;7,158,7} | 0,189 |
| 16 | $K_{10}$={5,9;77,8;125,6;113,0;53,6;89,3;166,9} | 0,108 |

a. *Fases $\phi_i$ expressas em graus. Atrasos $\tau_i$ normalizados em relação ao período do símbolo.*

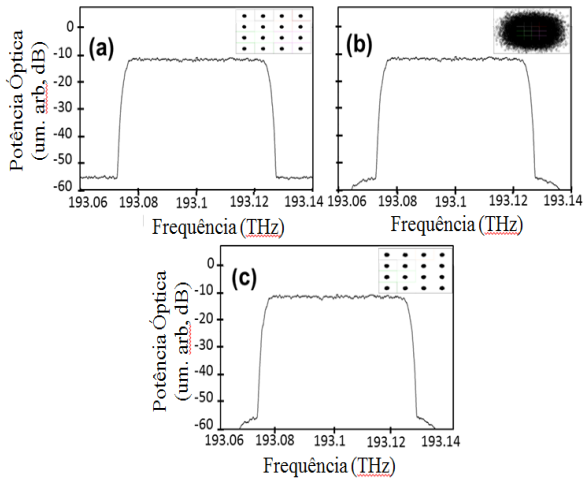


Fig. 5. Espectros e diagramas de constelação para a) o sinal QAM de entrada, b) o sinal codificado com $K_7$ e c) o sinal decodificado.

provida pelos processos de codificação e de decodificação observável a partir dos espectros das Figs. 4(a), 4(b) e 4(c).

## VI. Conclusões

Neste trabalho avaliou-se, no melhor de nosso conhecimento pela primeira vez na literatura, a utilização de um AG para a definição de chaves criptográficas para a técnica de criptografia óptica SPDE. O AG implementado produziu, para este relato, 3040 chaves para diferentes valores de $C$ e $M$, com um total de 9.2.3040 = 54720 chaves. Considerando-se todas as gerações, os percentuais médios de chaves geradas foram de ~93,37 e ~94,60% para taxas de mutação de, respectivamente, 5 e 4%.

Em situações práticas, um sistema utilizando a SPDE poderia ter uma grande base de chaves geradas pelo AG em questão e sortear, sempre que necessário, uma dessas para utilização. Existe naturalmente uma preocupação em como as chaves seriam enviadas do transmissor para o receptor. Uma abordagem detalhada desse problema é deixada para um trabalho futuro. Mas, por ora, menciona-se que essas chaves poderiam ser enviadas por outro canal ou no mesmo canal de comunicação e entre duas mensagens. Obviamente, em ambos os casos também é conveniente cifrar o sinal correspondente à chave. Isso pode ser feito, por exemplo, a partir esteganografia [12], ou, como a taxa de transmissão e o número de bits requeridos para transmitir a chave são baixos, a técnica QKD torna-se uma candidata muito interessante para a tarefa. A continuidade do trabalho abrange estratégias que permitam ao AG aumentar ainda mais o número de chaves válidas geradas e aplicar o algoritmo à situação em que as fatias espectrais sejam geradas por filtros com perfis não retangulares.

Por fim, destaca-se que uma grande vantagem da técnica avaliada é que as fases e os atrasos da chave podem variar continuamente. Isto permite a obtenção de um número bastante elevado de chaves [7]. Nota-se, no entanto, que as técnicas de criptografia na camada física, como a apresentada neste trabalho, complementam e não substituem a criptografia na camada de apresentação. De fato, quanto maior o número de camadas em que se realizar a codificação de dados/ sinais, mais seguro será o sistema de comunicação [13].

## Agradecimentos

Os autores agradecem ao CNPq (574017/2008-9, 311137/2014-8,), à FAPESP (08/57857-2) pelo financiamento do projeto no escopo do Programa Fotonicom. Os autores também agradecem à VPIPhotonics pelo provimento de licenças acadêmicas do *software* utilizado no trabalho relatado.

## Referências

[1] Research report: “2015 Cost of data breach study: global analysis,” Ponemon Institute, 2015.

[2] K. Shaneman and S. Gray,“Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention,” in Proc. MILCOM 2004—IEEE Military Communication Conference (IEEE, 2004), pp. 711–717, 2004.

[3] A.K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. 67, 661, August 1991.

[4] M. Cvijetic, I. Djordjevic, and A. Tanaka, “Quantum Communication Limits by Using Multichannel Spectral Space Scheme and Entangled Photons in Optical Fibers”, ICTON, 1-4, 2013.

[5] L. Zhang, X. Xin, B. Liu, and Y. Wang, "Secure OFDM-PON Based on Chaos Scrambling," IEEE Photonics Technology Letters, vol. 23, pp. 998-1000, July 2011.

[6] J.A. Cornejo, C.E. Perez, and J-L.B. Tocnaye, “Non-invasive WDM channel scrambling for secure high data rate optical transmissions,” IEEE/OSA Journal of Lightwave Technology, vol. 25, pp. 2081-2089, 2007.

[7] M.L.F. Abbade, L.A. Fossaluzza Junior, C.A. Messani, G.M. Taniguti, E.A.M. Fagotto, and I.E. Fonseca, “All-Optical Cryptography through Spectral Amplitude and Delay Encoding,” Journal of Microwaves, Optoelectronics and Electromagnetic Applications, v. 12, p. 376-397, 2013

[8] M.L.F. Abbade, M. Cvijetic, C.A. Messani, C.J. Alves, and S. Tenenbaum, “All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys,” Applied Optics, v. 54, p. 4359, 2015.

[9] M.L.F. Abbade, C.A. Messani, C.J. Alves, G.M. Taniguti, I. E. Fonseca, and E.A.M. Fagotto, “A new all-optical cryptography technique applied to WDM-compatible DPSK signals,” Proceedings of the 15th International Conference on Transparent Optical Networks- ICTON 2013, Cartagena- Espanha, paper We.B1.4, 2013.

[10] M.L.F. Abbade, M. Cvijetic, C.A. Messani, C.J. Alves, and S. Tenenbaum, “Double All-Optical Encryption of M-QAM Signals Based on Spectrally Sliced Encoding Keys,” Proceedings of the 17th International Conference on Transparent Optical Networks- ICTON 2015, Budapest- Hungria, paper Tu.A1.3, 2015.

[11] G. Mitsuo, C. Runwei, M. Gen, R. Chen, and L. Lin “Network Models and Optimization – Multiobjective Genetic Algorithm Approach”, Springer Verlag, 2008.

[12] B. Wu, Z. Wang, Y. Tian, M.P. Fok, B.J. Shastri, D.R. Kanoff, and P.R. Prucnal, "Optical steganography based on amplified spontaneous emission noise," Opt. Express 21, 2065-2071, 2013.

[13] K. I. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, “Security in photonic networks: threats and security enhancement,” J. Lightwave Technol., 29, 3210–3222, 2011.