Inteligência Computacional Aplicada à Criptologia: uma breve revisão

Moisés Danziger , Marco Aurélio Amaral Henriques (Orientador)

Departamento de Engenharia de Computação e Automação Industrial (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (Unicamp)
Caixa Postal 6101, 13083-970 – Campinas, SP, Brasil

{danziger,marco}@dca.fee.unicamp.br

Abstract – Many cryptographic techniques have been developed and several were broken. Recently, new models have arisen with different and more complex approaches, like those based on the Computational Intelligence (CI). Many bio-inspired techniques can be found in the literature showing their effectiveness in handling hard problems in the area of cryptology. However, some authors recognize that the advances have been slow and that more efforts are needed to take advantage of CI techniques. In this work, we present a brief review of some of the relevant works in this area. The main objective is to study the advantages of applying CI on cryptology and to find new ways of improving this approach to computer security.

Keywords – Artificial Neural Network, Evolutionary Computation, Artificial Immune Systems, Cryptology

1. Introdução

A criptologia é uma importante área da ciência. Ela é baseada na teoria dos números e na teoria da informação sendo composta por duas frentes interdependentes: a criptografia e a criptoanálise. Assim, um cifrador é um algoritmo criptográfico que usa funções específicas para cifrar e decifrar mensagens. Tais algoritmos são categorizados por dois tipos principais de chaves: simétricas e assimétricas [4]. Nos últimos anos muitos esquemas criptográficos foram criados e vários sofreram ataques. Um fator prepoderante nesses ataques é o crescimento do potencial computacional e das técnicas de criptoanálise. Por esse motivo há a necessidade de desenvolver sistemas criptográficos cada vez mais robustos.

A inteligência computacional (CI) tem como característica principal a habilidade em resolver problemas complexos, fato que facilita sua aplicação em criptologia. Na literatura, é possível encontrar várias técnicas de CI sendo aplicadas para resolver os mais variados problemas. Destacam-se as técnicas de computação evolutiva (EC) e redes neurais artificiais (ANN). Nosso objetivo é a investigação das vantagens e desvantagens da aplicaçao dessas técnicas sobre criptologia buscando novas linhas de pesquisa. Portanto, para melhor compreensão, dividimos o trabalho da seguinte forma: na seção 1 é apresentado um breve resumo sobre criptologia, seguido de um breve resumo das técnicas de CI na seção 2. Ainda na seção 2, nós apresentamos alguns estudos que apresentam potencial para nossa pesquisa. Finalmente, na seção 3 apresentamos uma discussão da aplicação de CI à criptologia e na seção 4 mostramos algumas conclusões.

2. Criptologia

Na Criptologia, a função básica da criptografia é a cifragem de uma mensagem (texto em claro) em outra mensagem (texto cifrado) de difícil compreensão caso seja interceptada por entidades não autorizadas [4]. Existem muitos tipos de algoritmos de cifragem/decifragem, porém, os mais utilizados são baseados em blocos como por exemplo, o DES - Data Encryption Standard - e o AES - Advanced Encryption Standard [5]. Ambos os algoritmos citados fazem parte do modelo criptográfico baseado em chaves simétricas. Existem ainda os algoritmos baseados em chaves assimétricas (isto é, existem duas chaves sendo uma pública e outra privada). Atualmente, as técnicas de CI têm sido adotadas para os dois modelos de algoritmos.

A análise de um sistema criptográfico é algo essencial para a criptologia. Portanto, a criptoanálise não existiria sem a criptografia [4]. A criptoanálise se utiliza de vários meios para investigar possíveis vulnerabilidades nos algoritmos criptográficos como por exemplo, criptoanálise diferencial e criptoanálise linear. De acordo com Joux [4], um bom algoritmo de criptografia precisa passar pelo crivo da criptoanálise. Todos os algoritmos criptográficos são vulneráveis a pelo menos um tipo de ataque: o ataque de força bruta no qual todas as possiveis chaves são testadas. Mas, este ataque esbarra

em um problema complexo: o tamanho do espaço de busca da chave o qual geralmente é tão grande que não é possível para um atacante tentar todas as possíveis chaves em um tempo aceitável. Abordagens bio-inspiradas têm sido usadas para analisar criptossistemas. Como princípio básico, o uso de CI nesse caso objetiva encontrar soluções que possam diminuir o tempo e a complexidade da busca da chave.

3. Inteligência Computacional e Criptologia

A inteligência computacional inclui várias áreas que são geralmente inspiradas por processos encontrados na natureza. Existem várias técnicas bio-inspiradas, porém, por questões de espaço, nesta seção não apresentaremos suas definições. Para isso, recomendamos o livro de inteligência artificial de Norvig e Russel [16]. Na literatura, encontramos vários trabalhos aplicando CI à criptologia. Porém, trataremos apenas alguns trabalhos considerados mais relevantes.

3.1. Redes Neurais Artificiais

Algumas das características mais importantes das ANNs (Artificial Neural Networks) derivam da sua estrutura paralela e sua inerente capacidade de se adaptar a problemas específicos [20]. Assim, guiados por estas habilidades, muitos pesquisadores tém aplicado ANN para criptografia. Por exemplo, Laskari et. al. [12] estudaram o desempenho das ANNs para resolver o problema do logaritmo discreto (DLP) e o problema da fatoração de inteiros grandes. Para o primeiro, os autores utilizaram uma rede neural recorrente (FNN) e, de acordo com as simulações realizadas, as FNNs alcançaram resultados satisfatórios para números primos pequenos. Porém, para números primos grandes o desempenho foi considerado bastante limitado. No caso do problema da fatoração de inteiros, os pesquisadores encontraram as mesmas dificuldades do DLP. Um fato importante é a necessidade de alterar as configurações (por exemplo, treinamento da FNN) conforme cresce a dificuldade do problema.

Liu e Guo [13] usaram redes neurais de Hopfield (HNN) com uma camada caótica (isto é, uma camada oriunda da teoria do caos usada para quebrar a linearidade, indesejável na criptografia) para desenvolver um criptosistema de chaves públicas. Segundo os autores, o modelo desenvolvido apresentou características que permitem o seu uso no contexto atual de criptografia (cifragem 50 vezes mais rápida que o RSA e robustez). Eles realizaram várias criptoanálises verificando que, pela dificuldade da decomposição de matrizes (bastante usada na teoria do caos) e das propriedades dos classificadores caóticos, o modelo apresenta índices satisfatórios de robustez. Há outra característica importante no modelo de Liu e Guo: o uso de processos diferentes para cifrar e decifrar. O resultado prático dessa técnica é o aumento da dificuldade para que atacantes possam encontrar a chave privada usando ataques do tipo “chosen-plaintext ”(um tipo de ataque bastante eficiente pois permite que o atacante escolha textos arbitrários para serem cifrados e obter os correspondentes textos cifrados) e “known-plaintext ”(nesse caso o atacante tem acesso ao texto cifrado e o texto plano de uma ou mais partes de dados).

Atualmente, as funções hash estão em evidência após vulnerabilidades encontradas nos padrões vigentes e, portanto, precisam de modelos mais robustos. Um exemplo de trabalho nesta linha pode ser visto em [22]. Lá, os autores apresentaram um modelo que gera um valor de hash com alta sensibilidade a mudanças na mensagem. Segundo os autores, ele é resistente aos ataques de força bruta e aniversário. Além desses atributos, eles afirmaram que o modelo é eficiente, prático e confiável, sendo um promissor candidato para funções hash (principalmente em plataformas de computação paralela).

3.2. Computação Evolutiva

Algoritmos naturais têm despertado interesse em muitas áreas da ciência [6]. Entre eles, o mais amplamente utilizado em criptologia são os algoritmos genéticos (GA), usados basicamente para criptoanálise. Mathews [18] e Spillman [19] podem ser considerados os pioneiros no uso de GA para criptoanálise. Ambos os autores publicaram trabalhos que utilizavam GA para atacar cifradores que usam substituição e transposição, além dos cifradores baseados no problema da mochila. Hernández et. al. [3] propuseram uma nova técnica de criptoanálise para o TEA (Tiny Encryption Algorithm) com número reduzido de rodadas (a redução do tamanho do problema para instâncias menores é

uma técnica bastante comum para abordagens iniciais do problema). Eles provaram que o uso de GA para distinguir um cifrador de bloco de uma permutação aleatória é possível. Nos trabalhos [2] e [9], Jonh propôs o algoritmo de busca tabu para criptoanálise e comparou várias técnicas, incluindo GA para quebra de criptosistemas clássicos. Mas, o autor também apresenta algumas limitações, afirmando que é preciso definir com muito cuidado os parâmetros dos algoritmos para que se possa encontrar boas soluções.

3.3. Autômato Celular

Em 1985, Stephen Wolfram propôs as primeiras idéias (teóricas) de CA para a criptografia [21]. Com o avanço do conhecimento sobre CA, novos trabalhos foram propostos e Guan [15] apresentou o primeiro modelo de criptosistema de chave pública usando CA. No modelo, a chave privada é usada como um conjunto de regras individuais na composição da função de cifragem. Para autenticidade, o autor usa uma função inversa da sua própria chave pública. Porém, a complexidade envolvida no desenvolvimento de um criptosistema baseado em CA é muita alta, sendo a questão da inversibilidade seu maior desafio. Bao [7] fez uma análise da segurança dos modelos que haviam sido propostos e mostrou que todos eram fortemente vulneráveis ao ataque "chosen-plaintext". Tal deficiência é decorrente da fragilidade do processo de geração das regras para o modelo CA criptográfico. Apesar de ter mostrado as deficiências, Bao também mostrou que, quando o conjunto de regras é bem analisado e criteriosamente escolhido, é possivel mitigar o problema. Assim, é possível aproveitar as vantagens dos CAs para uso em criptologia tais como, a facilidade em gerar padrões pseudo-aleatórios e a eficiência quando implementado em hardware.

3.4. Computação Baseada em DNA

Quando Leonard Adleman apresentou seu artigo seminal sobre a computação molecular (outro nome para computação baseada em DNA) [11], fez nascer novas perspectivas para os vários problemas difíceis de computação, como pôde ser visto no trabalho de Richard [17].

No campo da criptologia, Boneh et. al. [8] apresentaram um modelo teórico (matemático) para quebrar o DES. O modelo apresentado era genérico o suficiente para ser usado contra qualquer tipo de criptosistema que usasse chaves de até 64 bits. Por ser um trabalho pioneiro, ele evidenciou o potencial da computação DNA para criptoanálise de criptografia moderna. Recentemente, Tornea [14] apresentou dois algoritmos criptográficos baseados nas idéias dos algoritmos de chave pública e no princípio do "one-time pad"). Segundo o autor, os dois algoritmos podem ser embutidos em "microarrays", porém, o custo da tecnologia ainda é muito alto, inviabilizando testes reais. Mesmo assim, eles mostraram que é possível construir algoritmos criptográficos com alta segurança mostrando que esta é uma área bastante promissora.

3.5. Sistemas Imunológicos Artificiais

Baseados no sistema imunológico humano (HIS), essa abordagem da CI cresce rapidamente como um novo campo de pesquisa em inteligência artificial (AI). O HIS contém aspectos importantes, principalmente relacionados a sua capacidade de tratar problemas complexos e de forma distribuída. Entretanto, elas tem sido pouco empregadas em criptografia. Jacob et. al. [10] apresentaram um modelo de classificador imunológico com capacidade para detectar informações escondidas em imagems (técnica é conhecida como esteganografia). Os resultados alcançaram índices de até 91% de acerto usando sensores que nunca tinham sido expostos ao problema. Recentemente, Ali et. al. [1] aplicaram sistemas imunológicos artificiais (AIS) para atacar o DES, porém com apenas quatro rodadas.

4. Conclusão

Observando os trabalhos existentes na literatura, percebe-se que, apesar do potencial para aplicação de CI à criptologia, esta abordagem está caminhando. Existe uma grande dificuldade em trabalhar com as técnicas de CI para a representação do problema, ou seja, para mapear o problema computacionalmente. Porém, conforme disse John Clark [9], a comunidade de CI precisa se interessar mais pela criptografia. Comparando o uso das técnicas nós podemos observar que: (i) ANN e CA são usados principalmente para construir sistemas criptográficos, (ii) computação evolutiva e AIS são usados principalmente para criptonálise e (III) computação molecular tem sido aplicada para ambos os casos. Outra observação é a grande quantidade de artigos

usando ANN e GA em relação às outras abordagens. Como trabalhos futuros, estamos interessados na aplicação de AIS em criptologia. Nosso objetivo é comparar esta técnica com outras e avaliar seu potencial de maneira mais profunda, bem como avaliar o potencial da aplicação de CI a problemas de criptologia de um modo geral.

Referências

[1] Ali S.; Hamdani A.; Shafiq S.; Khan F. A. Cryptanalysis of four-rounded des using binary artificial immune system. volume 1, pages 338–346, 2010.

[2] Clark J. A. *Optimisiation Heuristics for Cryptology*. PhD thesis, Information Security Resarch Center, Faculty of Information Technology, Queensland University of Technology, 1998.

[3] Hernández J.; Sierra J.; Isasi P.; Ribagorda A. Genetic cryptanalysis of two rounds tea. *Lecture Notes in Computer Science*, 2331:1024–1031, 2002.

[4] Joux A. *Algorithmic cryptanalysis*. CRC Press series on cryptography and network security, 2009.

[5] Mollin R. A. *An Introduction to Cryptography - Second Edition*. Taylor and Francis Group, 2007.

[6] Goldberg D. E. *Genetic Algorithms in Search, Optimization and Machine Learning*. Addison-Wesley Publishing Company Inc., 1989.

[7] Bao F. Cryptanalysis of a new cellular automata cryptosystem. Number 2727, pages 416–427, 2003.

[8] Boneh D.; Dunworth C.; Lipton R. J. Breaking des using a molecular computer, 1995.

[9] Clark A. J. Invited paper. nature-inspired cryptography: Past, present and future. *Citeseer*, pages 1647–1654, 2003.

[10] Jacob T. J.; Gregg H. G.; Roger L. C. Jr.; Gary B. L. Novel steganofraphy detection using an artificial immune system approach, 2003.

[11] Adleman L. M. Molecular computation of solutions to combinatarial problems. *Science*, 11(266):1021–1024, 1994.

[12] Laskari E. C.; Meletiou G. C.; Tasoulis D. K.; Vrahatis M. N. Studying the performance of artificial neural networks on problems related to cryptography. *International Journal Nonlinear Analysis: Real World Applications*, (7):937–942, 2009.

[13] Liu N. and Guo D. Security analysis of public-key encryption scheme based on neural networks and its implementing. *International Conferences on Cybernetics and Intelligent Systems*, pages 443–450, 2006.

[14] Tornea O. Dna cryptography algorithms. pages 223–226. MEDITHEC, IFMBE, 2009.

[15] Guan P. Cellular automaton public-key cryptosystems. *Complex Systems*, 1(1):51–56, 1987.

[16] Russel S.; Norvig P. *Artificial Intelligence*. Person Education Inc., 1995.

[17] Lipton R. Using dna to solve np-complete problems. *Science*, 268:542–545, 1995.

[18] Mathews R. The use of genetic algorithms in cryptanalysis. *Cryptology*, 4(17):187–201, 1993.

[19] Spillman R. Cryptanalysis of knapsack ciphers using genetic algorithms. *Cryptology*, 4(17):367–377, 1993.

[20] Haykin S. *Neural Networks, A Comprehensive Foundation*. Prentice Hall, 1999.

[21] Wolfram S. Cryptography with cellular automata. In *LNCS*, pages 429–432. Advances in Cryptology, Springer-Verlag, 1986.

[22] Xiao D.; Liao X.; Wang Y. Parallel keyed hash function construction based on chaotic neural network. *International Journal of Neurocomputing*, (72):2288–2296, 2009.