As Contribuições Científicas de Diffie e Hellman - Prêmio Turing 2015

Seminário do Grupo de Grafos e Algoritmos da UFRJ

Luis Menasché Schechter
luisms@dcc.ufrj.br

Universidade Federal do Rio de Janeiro

20 de Julho de 2016

Whitfield Diffie e Martin Hellman

Whitfield Diffie e Martin Hellman (2)

Prêmio Turing

- Prêmio nomeado em homenagem ao matemático inglês *Alan Turing* (1912-1954)
- Turing é considerado um dos pais da Ciência da Computação
- Possui contribuições em teoria da computação, criptografia, computação científica, inteligência artificial e no desenvolvimento dos primeiros computadores de uso geral nas décadas de 40 e 50
- O *Prêmio Turing* é oferecido anualmente desde 1966 pela Association for Computing Machinery (ACM)
- O prêmio é acompanhado de um milhão de dólares para o vencedor (atualmente concedido pelo Google)
- É considerado o equivalente do Prêmio Nobel para a Computação
- Site do Prêmio Turing: `http://amturing.acm.org/`

Anúncio do Prêmio para Diffie e Hellman

"Whitfield Diffie e Martin Hellman são os recebedores do Prêmio Turing da ACM de 2015, pela sua contribuição crítica para a criptografia moderna. A habilidade de duas partes se comunicarem de forma privada sobre um canal inseguro é fundamental para bilhões de pessoas ao redor do mundo. De forma diária, indivíduos estabelecem conexões online seguras com bancos, sites de comércio eletrônico, servidores de e-mails e a nuvem. (continua)"

Anúncio do Prêmio para Diffie e Hellman (2)

"O revolucionário artigo de 1976 de Diffie e Hellman, 'New Directions in Cryptography' (Novas Direções na Criptografia), introduziu as ideias de criptografia de chave pública e assinaturas digitais, que são a fundação para a maioria dos protocolos de segurança usados regularmente na Internet atualmente. O protocolo Diffie-Hellman protege diariamente comunicações pela Internet e trilhões de dólares em transações financeiras."

(Tradução livre do anúncio da ACM)

Outros Vencedores Relacionados à Criptografia

- Manuel Blum - 1995
  - Premiado por contribuições em Teoria da Complexidade, estudo de aleatoriedade e geradores de números pseudo-aleatórios e suas aplicações à criptografia e verificação de programas
  - Contribuiu no estudo de *commitment protocols*, desenvolvendo um protocolo para um jogo de cara-e-coroa honesto por telefone
  - Desenvolveu diversos geradores de números pseudo-aleatórios criptograficamente seguros
  - Desenvolveu o sistema de criptografia Blum-Goldwasser
  - É um dos desenvolvedores do CAPTCHA
  - Foi orientador de doutorado de Leonard Adleman (P.T. 2002), Shafi Goldwasser (P.T. 2012), Silvio Micali (P.T. 2012), Michael Sipser, Luis von Ahn (criador do reCAPTCHA), Umesh e Vijay Vazirani e Ivan da Costa Marques (DCC/UFRJ), entre outros.
  - Foi orientado de Marvin Minsky (P.T. 1969)

Outros Vencedores Relacionados à Criptografia (2)

- Andrew Chi-Chih Yao - 2000
  - Premiado por contribuições em Teoria da Computação, incluindo estudos em Teoria da Complexidade, geração de números pseudo-aleatórios, criptografia e complexidade de comunicação
  - Estudou algoritmos randomizados e formas de medir sua complexidade
  - Desenvolveu o modelo Dolev-Yao, um modelo formal para a verificação de protocolos de segurança
  - Estudou geradores de números pseudo-aleatórios criptograficamente seguros
  - Desenvolveu o Teste de Yao para sequências pseudo-aleatórias
  - Estudou o Problema dos Milionários de Yao, onde dois milionários querem saber qual dos dois é mais rico sem revelarem suas respectivas riquezas
  - Desenvolveu a ideia de circuitos ilegíveis (*garbled circuits*), utilizados em protocolos de comunicação segura
  - Estudou circuitos quânticos, computação quântica e comunicação quântica

Outros Vencedores Relacionados à Criptografia (3)

- Ronald Rivest, Adi Shamir e Leonard Adleman - 2002
  - Premiados pela importante contribuição de tornar a ideia de criptografia de chave pública útil na prática
  - Desenvolveram o algoritmo RSA de criptografia e assinatura em 1977, o mais utilizado na Internet até hoje
  - Fundaram a empresa RSA Data Security (vendida em 2006 por 2 bilhões de dólares), que originou diversas outras empresas de segurança, incluindo a Verisign
  - Rivest é co-autor de um dos livros mais conceituados de teoria de algoritmos e estruturas de dados: Introduction to Algorithms (Algoritmos - Teoria e Prática)
  - Rivest estuda também sistemas de votação seguros, tendo proposto alguns protocolos de votação como o ThreeBallot

Outros Vencedores Relacionados à Criptografia (4)

- Ronald Rivest, Adi Shamir e Leonard Adleman - 2002 (cont.)
  - Shamir estudou e desenvolveu protocolos de conhecimento zero, desenvolveu um método de criptoanálise conhecido como criptoanálise diferencial, desenvolveu protocolos de compartilhamento de segredos, desenvolveu métodos de criptografia baseados em identidade (*identity-based*) e métodos de criptografia visuais
  - Adleman desenvolveu alguns testes de primalidade e é um dos pioneiros na área de *DNA Computing* / Computação Molecular

Outros Vencedores Relacionados à Criptografia (5)

- Shafi Goldwasser e Silvio Micali - 2012
  - Premiados por suas contribuições em Teoria da Computação, Criptografia e Teoria da Complexidade
  - Desenvolveram o conceito de encriptação probabilística (e sua aplicação em *commitment protocols*)
  - Desenvolveram o conceito de sistemas interativos de prova
  - Desenvolveram o conceito de provas de conhecimento zero (*zero-knowledge proofs*)
  - Desenvolveram o método de criptografia Goldwasser-Micali
  - Goldwasser desenvolveu o método de criptografia Blum-Goldwasser
  - Goldwasser desenvolveu o método de criptografia GGH (Goldreich-Goldwasser-Halevi)
  - Micali estudou métodos para a geração de sequências de números pseudo-aleatórios
  - Micali estudou provas de conhecimento zero para problemas em NP

Whitfield Diffie - Breve Biografia

- Nasceu em Washington, D.C. (EUA), em 1944
- Realizou graduação em Matemática no MIT (EUA)
- Não realizou pós-graduação
- Trabalhou no sistema de computação algébrica MATHLAB (atual Macsyma)
- Trabalhou na ARPAnet
- Foi Chief Security Officer da Sun Microsystems

Martin Hellman - Breve Biografia

- Nasceu em Nova York (EUA) em 1945
- Realizou graduação em Engenharia Elétrica na Universidade de Nova York (EUA)
- Realizou pós-graduação em Engenharia Elétrica em Stanford (EUA)
- Seu orientador de doutorado foi Thomas Cover
- Foi orientador de doutorado de Taher El Gamal, Ralph Merkle e Stephen Pohlig
- Professor de Stanford desde 1969, tornando-se Professor Emérito em 1996

Outros Prêmios Recebidos por Diffie e Hellman

- Prêmio EFF Pioneer Award em 1994
- Prêmio Kanellakis em 1996 (com Rivest, Shamir, Adleman e Merkle)
- Prêmio do Jubileu de Ouro do IEEE Information Theory Society em 1998
- Prêmio Marconi em 2000
- Medalha Hamming do IEEE em 2010 (com Merkle)

Principais Contribuições Conjuntas de Diffie e Hellman

- Invenção do conceito de Criptografia de Chave Pública
- Invenção do conceito de Assinatura Digital
- Algoritmo de acordo de chave (*key-agreement*) Diffie-Hellman

- Artigo "New Directions in Cryptography", IEEE Transactions on Information Theory 22(6), 644-654, 1976
- "We stand today on the brink of a revolution in cryptography."

Outras Contribuições

- Método de critografia de chave pública Merkle-Hellman, que utiliza como problema matemático subjacente o problema da mochila (Hellman e Merkle)
  - Artigo "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Transactions on Information Theory 24(5), 525-530, 1978
- Algoritmo Pohlig-Hellman para a resolução do problema do logaritmo discreto (Hellman e Pohlig)
  - Artigo "An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance", IEEE Transactions on Information Theory 24(1), 106-110, 1978

Criptografia de Chave Privada

- Alice quer enviar uma mensagem criptografada para Bernardo através de um canal inseguro
- Alice e Bernardo devem entrar em acordo a respeito de uma chave privada a ser utilizada nos processos de encriptação e decriptação da mensagem.
- Este acordo pode ser feito utilizando-se um segundo canal, sendo este um canal seguro ou
- Ambos podem utilizar uma terceira parte confiável (*trusted-third-party* ou TTP) para fornecer a eles a chave
- Problemas óbvios:
  1. Se o canal original é inseguro, significa que não há facilidade em se obter um canal seguro
  2. Não se encontra uma TTP em cada esquina

Criptografia de Chave Pública

- Alice quer enviar uma mensagem criptografada para Bernardo através de um canal inseguro
- Bernardo possui uma chave pública de codificação e uma chave privada de decodificação
- Qualquer um (incluindo Alice) pode utilizar a chave pública de Bernardo para codificar mensagens destinadas a ele antes de enviá-las
- Apenas Bernardo pode decodificar (com sua chave privada) tais mensagens e acessar seu conteúdo original
- Calcular a chave privada a partir do conhecimento da chave pública deve ser um problema computacionalmente difícil
- O cálculo da chave privada envolve algum problema matemático subjacente que possui alta complexidade computacional (NP)
- Exemplos de problemas matemáticos subjacentes: fatoração de inteiros, logaritmo discreto

Assinatura Digital

- Alice quer enviar uma mensagem assinada para Bernardo
- Alice possui uma chave privada de assinatura e uma chave pública de verificação
- Qualquer um (incluindo Bernardo) pode utilizar a chave pública de Alice para verificar a assinatura ao receber mensagens enviadas por ela
- Apenas Alice pode assinar corretamente (com sua chave privada) as mensagens
- As mesmas considerações a respeito do cálculo da chave privada a partir do conhecimento da chave pública se aplicam neste caso

O Algoritmo Diffie-Hellman

- O algoritmo Diffie-Hellman é um algoritmo de *key-agreement*
- Seu objetivo é que duas partes desejando utilizar um protocolo de criptografia de chave *privada* consigam entrar em acordo apenas através de comunicações em um canal *inseguro* a respeito do valor da chave a ser utilizada
- O uso deste algoritmo remove a necessidade de um canal secundário seguro
- Selecionamos inicialmente um número primo p
- Consideramos o conjunto $U(p) = \{1, 2, \ldots, p-1\}$
- O *Teorema da Raiz Primitiva* nos garante que existe um elemento $g \in U(p)$ tal que todos os elementos de $U(p)$ podem ser escritos como potências de g módulo p. Isto é, $U(p) = \{1, g, g^2, g^3, \ldots, g^{p-2}\} \pmod{p}$

O Algoritmo Diffie-Hellman (2)

- Alice escolhe um inteiro $1 \leq a \leq p-2$ e Bernardo escolhe um inteiro $1 \leq b \leq p-2$
- Alice calcula $c = g^a \bmod p$ e Bernardo calcula $d = g^b \pmod p$
- Alice envia c para Bernardo e Bernardo envia d para Alice
- Alice calcula $e = d^a \bmod p$ e Bernardo calcula $f = c^b \bmod p$
- Temos que

$$e \equiv d^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv c^b \equiv f \pmod p$$

- O valor $e = f$ será usado como chave por Alice e Bernardo

O Algoritmo Diffie-Hellman (3)

- Os valores que trafegam no canal são g^a e g^b.
- Para usar estes valores para calcular a chave g^{ab}, o atacante precisaria extrair o valor de a ou de b de um dos valores que trafegaram no canal
- Mas para isso seria necessária uma maneira eficiente de se resolver o problema do logaritmo discreto

As Contribuições Científicas de Diffie e Hellman - Prêmio Turing 2015

Seminário do Grupo de Grafos e Algoritmos da UFRJ

Luis Menasché Schechter
luisms@dcc.ufrj.br

Universidade Federal do Rio de Janeiro

20 de Julho de 2016