1 PRINCIPAIS TRABALHOS PUBLICADOS

1.1 Trabalhos com avaliadores, publicados em anais ou revistas técnicas internacionais

Observamos que:

a) [1] é citado em vários artigos internacionais e no livro "The Traveling Salesman Problem", por E. L. Lawler, editado por John Wiley and Sons, em 1983.

b) [7] é citado no artigo "Differential Cryptanalysis of Lucifer", por E. Biham, no Proc. of CRYPTO'93, Lecture Notes in Computer Science, editado por Springer-Verlag, em 1993, e no livro Applied Cryptography (2nd. edition), por B. Schneier, editado por John Wiley and Sons, em 1995.

c) [16] e [13] são citados no artigo "Adaptive reconstructive τ openings: convergence and the steady-state distribution", por Yidong Chen and Edward R. Dougherty, Journal of Electronic Imaging, July 1996, vol. 5, number 3, pp 266-282.

Referências

[1] Routo Terada and John Halton. A Fast Algorithm for the Euclidean Traveling Salesman Problem, Optimal with Probability One. *SIAM Journal on Computing.* vol. 11, no. 1, fevereiro de 1982, 19 pgs.

[2] Routo Terada. An optimal algorithm for set packing and its analysis. In Fred S. Roberts, editor, *Proc. Third SIAM Conference on Discrete Mathematics – Clemson University, S. Carolina*, page A20, E.U.A., 1986. Society for Industrial and Applied Math., 11 pgs.

[3] Routo Terada. Probabilistic analysis of optimal algorithms for three NP-hard problems. In K. Tanabe, editor, *Proc. 13th. International Symposium on Mathematical Programming*, Tokyo, 1988, 16 pgs. Chuo University – Japan.

[4] Routo Terada. A cryptographic function based on majority circuits. Technical Group On Information Security – IEICE, Nihondaira, Japão Proc. of the Symp. of Cryptography and Information Security, Jan. 31-Feb. 2, 1990, Japan, 13 pgs.

[5] Routo Terada. A cryptographic function based on majority circuits. *Transactions of the Institute of Electronics, Information, and Communication Engineers – Japan*, E73:1036–1040, 1990, 5 pgs.

[6] Kenji Koyama and Routo Terada. Nonlinear parity circuits and their cryptographic applications. In *Lecture Notes in Computer Science – CRYPTO'90, Springer-Verlag*, pages 582–599, 1991. vol. 537, 10 pgs., International Association for Cryptographic Research – IACR.

[7] Kenji Koyama and Routo Terada. How to strengthen DES like cryptosystems against Differential Cryptanalysis. *Transactions of the Institute of Electronics, Information, and Communication Engineers, Japan*, pages 63-69, 1993, 6 pgs.

[8] Kenji Koyama and Routo Terada. Probabilistic swapping schemes to strengthen DES against differential cryptanalysis. In *Proc. of the Symp. of Cryptography and Information Security, Jan. 28-30 1993, Japan.* Institute of Electronics, Information, and Communication Engineers – Japan, 1993.

[9] Toshinobu Kaneko and Kenji Koyama and Routo Terada. Dynamic swapping schemes and differential cryptanalysis. In *Proc. of the 1993 Korea-Japan Joint Workshop on Information Security and Cryptology (Oct. 24-26, 1993)*, pages 292–301. Institute of Electronics, Information, and Communication Engineers – Japan, 1993.

[10] Toshinobu Kaneko and Kenji Koyama and Routo Terada. Dynamic swapping schemes and differential cryptanalysis. *Transactions of the Institute of Electronics, Information, and Communication Engineers, Japan*, pages 1328-1336, 1994, 9 pgs.

[11] Routo Terada and Paulo Geraldo Pinheiro. How to strengthen FEAL against Differential Cryptanalysis. In *Proc. of the 1995 Korea-Japan Joint Workshop on Information Security and Cryptology (January 24-27, 1995)*, pages V–1.1– V1.10. Institute of Electronics, Information, and Communication Engineers – Japan, 1995.

[12] Y. Nakao and T. Kaneko and K. Koyama and R. Terada. A study on the security of RDES cryptosystem against Linear Cryptanalysis. In *Proc. of the 1995 Korea-Japan Joint Workshop on Information Security and Cryptology (January 24-27, 1995)*, pages V–2.1– V2.10. Institute of Electronics, Information, and Communication Engineers – Japan, 1995.

[13] J. Barrera and N. S. Tomita and F. S. C. Silva and R. Terada. Automatic programming of binary morphological machines by PAC learning. In *1995 Intn'l Symp. on Optical Science, Eng., and Instrumentation*, 9-14 July 1995, San Diego, California. organizado pelo SPIE – Intn'l Society for Optical Engineering.

[14] Routo Terada and Paulo Geraldo Pinheiro and Kenji Koyama. A new version of FEAL, stronger against Differential Cryptanalysis. *Transactions of the Institute of Electronics, Information, and Communication Engineers – Japan*, E79-A(1):28–34, January 1996.

[15] Y. Nakao and T. Kaneko and K. Koyama and R. Terada. The security of RDES cryptosystem against Linear Cryptanalysis. *Transactions of the Institute of Electronics, Information, and Communication Engineers – Japan*, E79-A(1):12–19, January 1996.

[16] Junior Barrera, Routo Terada, Flavio S C Silva, and Nina S Tomita. Automatic programming of MMach's for OCR. In P. Maragos, editor, *Mathematical Morphology and its applications to Signal and Image Processing*. Kluwer Academic Publishers, May 1996.

[17] R. Terada and Jorge Nakahara Jr. Linear and differential cryptanalysis of FEAL-N with swapping. 1997 Internat'l Symposium on Computer and Information Security, Fukuoka, Japan.

[18] K. Koyama and R. Terada. An augmented family of Cryptographic Parity Circuits. 1997 Information Security Worshop, Ishikawa, Sep 17-19, 1997, Japan, In Lec. Notes in Comp. Sci. no. 1396, pp 198-208, Springer-Verlag.

[19] J. Barrera and R. Terada et al. An OCR based on Morphological Operators In *10th Annual Symp. on Electronic Imaging*, January 24 - 29, 1998, San Jose, California. organizado pelo SPIE – Intn'l Society for Optical Engineering.

[20] J. Barrera and R. Terada et al. Automatic Programming of Morphological Machines by PAC Learning *Fundamenta Informatikae*, vol 43, Numbers 1,2 January 2000, pp. 229-258 (EATCS - IOS Press).

[21] J. Barrera, M. Brun, R. Terada and E. R. Dougherty Boosting OCR Classifier by Optimal Edge Noise Filtering. In *12th Annual Symp. on Electronic Imaging*, January, 2000, San Jose, California. organizado pelo SPIE – Intn'l Society for Optical Engineering.

[22] R. Terada and Paulo G. Pinheiro Quadratic relations for S-boxes. In Information Security Conference, October 1-3, 2001, Malaga, Spain Lecture Notes in Computer Science number 2200, Springer-Verlag. pp 294-309.

[23] R. Hirata and J. Barrera and R. Terada and E. Dougherty The incremental splitting of intervals algorithm for the design of binary image operators. In International Symp. of Mathematical Morphology, April, 2002, Sydney, Australia Proceedings, Kluwer Publishing organizado pelo SPIE – Intn'l Society for Optical Engineering

[24] R. Terada and I. Correa Jr., A stronger version of RC6 against differential cryptanalysis. In Symposium on Computer and Information Security, February 2003, Hamamatsu, Japan. Proceedings of SCIS 2003, organizado pelo IEICE – Institute of Electronics, Information, and Communication Engineers – Japan

[25] R. Terada and W. Benits Jr. and E. Okamoto, An IBE Scheme to exchange authenticated secret keys. In Symposium on Computer and Information Security, February 2004, Sendai, Japan. Proceedings of SCIS 2004, pp 4C205-4C209, organizado pelo IEICE – Institute of Electronics, Information, and Communication Engineers – Japan

[26] R. Terada and Denise H Goya, A Certificateless Public Key Encryption based on Bilinear Pairing Functions. In Symposium on Computer and Information Security, February 2006, Hiroshima, Japan. Proceedings of SCIS 2006, pp 2A2-2-1 - 2A2-2-6 organizado pelo IEICE – Institute of Electronics, Information, and Communication Engineers – Japan

[27] R. Terada and Denise H Goya, A Certificateless Signature Scheme based on Bilinear Pairing Functions, In Symposium on Computer and Information Security, February 2007, Sasebo, Japan. Proceedings of SCIS 2007, pp 2C4-5-1 - 2C4-5-7 organizado pelo IEICE – Institute of Electronics, Information, and Communication Engineers – Japan

[28] R. Terada and Eduardo T. Ueda, A new version of the RC6 algorithm, stronger against chi^2 cryptanalysis, In Proc. of the 7th Australasian Information Security Conference (AISC 2009), Wellington, New Zealand, pp 47-52.

1.2 Trabalhos com avaliadores, publicados em anais ou revistas técnicas nacionais

Referências

[1] Routo Terada. Senhas Criptografadas, com Assinatura Eletrônica. Anais do XVI Congresso Nacional de Informática, São Paulo, 1983;

[2] Routo Terada. Criptografia para usuários em ATM. In *Anais do VII Congresso Nacional de Auditores Internos*, 1984.

[3] Routo Terada. Um Esquema de Criptografia para Autenticação de Usuários. *Anais do XVII Congresso Nacional de Informática*, 1984.

[4] Routo Terada. Complexidade de Detecção de Procedimentos Recursivos. *Anais do 14 Coloquio Brasileiro de Matemática*, Poços de Caldas.

[5] R. Terada. Algoritmos rápidos para ordenação em paralelo. In *X Congresso Nacional de Matemática Aplicada e Computacional*. SBMAC, setembro 1987.

[6] R. Terada. Aplicações de assinatura digital em integridade de documentos eletrônicos. In SUCESU, editor, *XX Congresso Nacional de Informática*, setembro 1987.

[7] R. Terada. Classes de computação paralela e exemplos de problemas que admitem algoritmos paralelos rápidos. In *I Simpósio de Arquitetura de Computadores*. Sociedade Brasileira de Computação, maio 1987.

[8] R. Terada. Soluções 'zero-knowledge' para problemas de identificação criptográfica. In *Anais do XXI Congresso Nacional de Informática*, pages 781–783, 1988.

[9] Routo Terada. Segurança na redes de comunicação de dados. In *Anais do I Congresso Nacional de Auditoria e Segurança de Informação*, SUCESU-SP, S. Paulo, 1988, 17 pgs.

[10] Routo Terada. Uma identificação criptográfica compacta do tipo zero-knowledge. In *Anais da Secretaria Especial de Informática – Brasília*, 1989. 6p.

[11] Routo Terada. Um circuito criptográfico e aplicações. In P. Feldman, editor, *XXV Congresso Nacional de Informática*, pages 641–648, Rua Tabapuã, São Paulo, 1991. SUCESU.

[12] N. Hirata and J. Barrera and R. Terada. Text Segmentation by Automatically Designed Morphological Operators *SIBGRAPI – Simpósio Brasileiro de Comp. Gráfica e Processamento de Imagem, 2000*

[13] R. Terada and Vilc Q. Rufino, Correção de Deficiências no Acordo de Chaves de Mandt, In Anais do IX Simpósio Brasileiro em Segurança da Informação de Sistemas Computacionais (UNICAMP, 2009) pp 101-114.

[14] Denise H. Goya and R. Terada and Vilc Q. Rufino, Acordo de Chave sem Certificados sob Emissão Múltipla de Chaves Públicas (short paper), In Anais do IX Simpósio Brasileiro em Segurança da Informação de Sistemas Computacionais (UNICAMP, 2009) pp 241-242.

1.3 Teses

Referências

[1] Routo Terada. Um Código Criptográfico em Transmissão e Base de Dados. Tese de Livre-Docência, junho de 1987, IME-USP;

[2] Routo Terada. Fast Probabilistic Algorithms for NP-hard Problems, which are Optimal with Probability One. Tese de doutoramento, University of Wisconsin-Madison, 1979.

[3] Routo Terada. Linguagens Determinísticas. Dissertação de mestrado, IME-USP, 1975.

1.4 Livros e textos didáticos

Referências

[1] Denise H. Goya, Mehran Misaghi, Vilc Rufino, R. Terada. *MODELOS DE CRIPTOGRAFIA DE CHAVE PÚBLICA ALTERNATIVOS.* In Anais do IX Simpósio Brasileiro em Segurança da Informação de Sistemas Computacionais (UNICAMP, 2009) pp 49-98.

[2] R. Terada. *DESENVOLVIMENTO DE ALGORITMOS E COMPLEXIDADE DE COMPUTAÇÃO.* Terceira Escola de Computação, PUC-Rio de Janeiro, julho de 1982, 231 páginas.

[3] R. Terada and Valdemar Setzer. *INTRODUÇÃO À COMPUTAÇÃO E À CONSTRUÇÃO DE ALGORITMOS.* DCC-IME-USP, 1986.

[4] R. Terada. *INTRODUÇÃO À COMPLEXIDADE DE ALGORITMOS PARALELOS*. VII Escola de Computação, IME-USP, julho 1990, 231 pgs.

[5] R. Terada and V.W. Setzer. *INTRODUÇÃO À COMPUTAÇÃO E À CONSTRUÇÃO DE ALGORITMOS*. Editora McGraw-Hill Ltda., São Paulo, 1991.

[6] Routo Terada. *DESENVOLVIMENTO DE ALGORITMOS E ESTRUTURAS DE DADOS*. McGraw-Hill do Brasil, Rua Tabapuã – S.Paulo, 1991.

[7] Routo Terada and Julio Stern. *GUIA DE PROGRAMAÇÃO EM C: Vade MeCum* publicado pelo DCC-IME-USP, 1994.

[8] R. Terada. *Segurança de Dados – Criptografia em Redes de Computador*. Editora Blücher, São Paulo, 242 páginas, 2000.

1.5 Trabalhos de divulgação, sem avaliadores

Referências

[1] R. Terada. RFXDHCVFPUPSC ou não Criptografado. *Revista Informática e Administração*, ano 1, no. 10, páginas 20 a 23, 1985.

[2] R. Terada. Criptografia, segredo contra a violação de dados. *Data News*, Ano XI, número 383, outubro de 1987, p. 16-18.

[3] R. Terada. Criptografia: a chave da segurança. *Atuação*, 1(5), 1988.

[4] R. Terada. Criptografia e a importância de suas aplicações. *Revista do Professor de Matemática*, 12:1–7, 1988. SBM+IMEUSP.

[5] R. Terada. O estado da arte em segurança de informações sensíveis. *DCI-Informática*, 27 junho 1988.

[6] R. Terada. O detetor de vírus. *Jornal de Software*, (4), abril, 1989, 2 pgs.

[7] R. Terada. Mensagem viaja disfarçada. *Caderno de Informática do Jornal da Tarde*, maio 1995.

1.6 Revisão técnica e/ou tradução de livros

1. Tradução do livro "Basic Computer Programming", Bartee, para a Editora Harper do Brasil, 1985, 368 pg.;

2. Revisão técnica do livro "First Publisher", da Software Publishing Corporation, 1989, 212 pg.;

3. Revisão técnica do livro "Sistemas de Bancos de Dados"para a Editora McGraw-Hill do Brasil, 1989, 582 pg.;

2 LISTA DE PATENTES OBTIDAS E/OU PENDENTES

Patente do circuito criptográfico no artigo:

Referências

[1] Kenji Koyama and Routo Terada. Nonlinear parity circuits and their cryptographic applications. In *Lecture Notes in Computer Science – CRYPTO'90, Springer-Verlag*, pages 582–599, 1991. vol. 537.

3 LISTA DE RESULTADOS DE PESQUISA TRANSFERIDOS E ADOTADOS PELO SETOR PRODUTIVO

1. Software (para Windows-NT) de reconhecimento de caracteres impressos - OCR - desenvolvido pelo Projeto VERASS e adotado pela Olivetti do Brasil, em 1995/96;

2. Software (para Windows-NT) de detecção de falhas em circuito impresso, desenvolvido pelo Projeto VERASS e adotado pela Olivetti do Brasil, em 1995/96;