Publications du LACS 2005-2006 (extrait)

Livres ou chapitres de livres

A. Biryukov: **30 articles** in Encyclopedia of Cryptography and Security (Hardcover) by Henk C.A. van Tilborg (Editor) Springer, 53 pages, August 2005.

F. Leprévost, T. Ebrahimi et B. Warusfel (éditeurs). **La sécurité Multimédia volumes 1 & 2**, Hermès, 2006

P. Bouvry, J.-G. Dumas, R.Gillard, J.-L. Roch and S. Varrette. Sécurité Multimédia: Cryptographie et Sécurité Systèmes et Réseaux. (vol. 2), chapitre: "**Cryptographie à Clef Secrète**", T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 23--99, Hermès publishing, Fev 2006.

J.-G. Dumas, F. Leprévost, J.-L. Roch, V. Savin and S. Varrette. Sécurité Multimédia: Cryptographie et Sécurité Systèmes et Réseaux. (vol. 2), chapitre: "**Cryptographie à Clef Publique**", T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 103--182, Hermès publishing, Fev 2006.

J.-G. Dumas, F. Leprévost, J.-L. Roch and S. Varrette. Sécurité Multimédia: Cryptographie et Sécurité Systèmes et Réseaux. (vol. 2), chapitre: "**Architectures PKI**", T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 187--208, Hermès publishing, Fev 2006.

N. Bernard, Y. Denneulin and S. Varrette. Sécurité Multimédia: Cryptographie et Sécurité Systèmes et Réseaux. (vol. 2), chapitre: "**Sécurité UNIX**", T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 211--241, Hermès publishing, Fev 2006.

N. Bernard, P. Bouvry, Y. Denneulin and S. Varrette. Sécurité Multimédia: Cryptographie et Sécurité Systèmes et Réseaux. (vol. 2), chapitre: "**Sécurité Réseaux**", T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 247--295, Hermès publishing, Fev 2006.

T. Ebrahimi, F. Leprévost, B. Warusfel. Sécurité Multimédia: Enjeux de la Sécurité. (vol. 1), chapitre : « **Réalités de l'espionnage industriel** », T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 211--241, Hermès publishing, Fev 2006.

J.-C. Asselborn. Sécurité Multimédia: Enjeux de la Sécurité. (vol. 1), chapitre : « **Introduction générale à la cryptographie et à ses applications dans la société de l'information** », T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 211--241, Hermès publishing, Fev 2006.

J.-S. Coron et L. Goubin. Sécurité Multimédia: Enjeux de la Sécurité. (vol. 1), chapitre : « **Cartes à puce** », T. Ebrahimi and F. Leprévost and B. Warusfel editor, pages 211--241, Hermès publishing, Fev 2006.

Articles

Alex Biryukov, Adi Shamir, **Analysis of the Non-linear Part of Mugi**. FSE 2005: 320-329

Jongsung Kim, Alex Biryukov, Bart Preneel, Sangjin Lee, **On the Security of Encryption Modes of MD4, MD5 and HAVAL**. ICICS 2005: 147-158

Alex Biryukov, Sourav Mukhopadhyay, Palash Sarkar, **Improved Time-Memory Trade-Offs with Multiple Data**. Selected Areas in Cryptography 2005: 110-127

Hirotaka Yoshida, Alex Biryukov, **Analysis of a SHA-256 Variant**. Selected Areas in Cryptography 2005: 245-260

Alex Biryukov, Joseph Lano, Bart Preneel, **Recent attacks on alleged SecurID and their practical implications**. Computers & Security 24(5): 364-370 (2005)

Eli Biham, Alex Biryukov, Adi Shamir, **Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials**. J. Cryptology 18(4): 291-311 (2005)

C. De Cannière, A.Biryukov, B.Preneel, **An Introduction to Block Cipher Cryptanalysis**, Special Issue of the journal "Proceedings of the IEEE" on Cryptography and Security, 10 pages, Autumn 2005.

H.Yoshida, A. Biryukov, B. Preneel, **Some Applications of the Biham-Chen attack**, electronic proceedings of ECRYPT Hash function, Krakow, Poland and NIST Cryptographic Hash Function Workshop, USA, 2005, 10 pages.

A.Biryukov, **A New 128-bit Key Stream Cipher: LEX**, electronic proceedings of SKEW'2005 workshop, Aarhus, Denmark, May 2005, 7 pages.

Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, Prashant Puniya, **Merkle-Damgard revisited: how to build a hash function**, CRYPTO 2005

Jean-Sébastien Coron, David Lefranc, Guillaume Poupard, **A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis**, CHES 2005

Julien Cathalo, Jean-Sébastien Coron, David Naccache, **From Fixed-Length to Arbitrary-Length RSA Encoding Schemes Revisited** , PKC 2005.

Sébastien Varrette, Jean-Louis Roch, Johan Montagnat, Ludwig Seitz, Jean-Marc Pierson and Franck Leprévost. **Safe Distributed Architecture for Image-based Computer Assisted Diagnosis**. In: IEEE 1st International Workshop on Health Pervasive Systems (HPS'06), Lyon, France, june 2006.

Sébastien Varrette, Sébastien Georget, Johan Montagnat, Jean-Louis Roch and Franck Leprévost. **Distributed Authentication in GRID5000**. LNCS 3762, R. Meersman and al. editor, In: LNCS OnTheMove Federated Conferences - Workshop "Grid Computing

and its Application to Data Analysis (GADA'05)", pages 314--326, Springer Verlag publishing, Agia Napa, Cyprus, November 1 2005.

Nathalie Dagorn, Nicolas Bernard and Sébastien Varrette. **Practical Authentication in Distributed Environments**. IEEE editor, In: IEEE International Computer Systems and Information Technology Conference (ICSIT'05), Sheraton Hotel, Alger, July 19--21 2005.

Nathalie Dagorn, and N. Bernard. **Web Hacking**. In Proceedings of the fourth IADIS International Conference on the World Wide Web and the Internet (WWW/Internet 2005), Oct. 2005.

Franck Leprévost, Jean Monnerat, Sébastien Varrette and Serge Vaudenay. **Generating Anomalous Elliptic Curves**. Journal: Information Processing Letters (93), pages 225--230, Elsevier Science publishing, 2005.

Sébastien Varrette, Sébastien Georget, Jean-Louis Roch and Franck Leprevost. **Authentification Distribuée sur Grille de Grappes basée sur LDAP**. In: Proceedings des 16èmes rencontres francophones du parallélisme (RenPar'16), Le Croisic, France, April 6--8 2005.

Axel Krings, Jean-Louis Roch, Samir Jafar and Sébastien Varrette. **A Probabilistic Approach for Task and Result Certification of Large-scale Distributed Applications in Hostile Environments**. LNCS 3470, Springer Verlag editor, In: Proceedings of the European Grid Conference (EGC2005), Springer Verlag publishing, Amsterdam, Netherlands, February 14--16 2005.

Organisation de Conférences et participation à des comités de programmes (extrait)

CAiSE '06

SECRYPT 2006

CT-RSA'05 (US)
CRYPTO'05 (US)
ASIACRYPT'05 (India)
ICICS'05 (China)
ICISC'05 (Korea)
Indocrypt'05 (India)
ISC'06 (Greece)
SAC'05 (Canada)
EUROCRYPT'06 (Russia)
ICISC'06 (Korea)
Benelux WISS'06 (Belgium)