

4. APPENDIX

DETAILED REPORT OF MODULES 1 AND 3 RESEARCH RESULTS, REFERENCES AND OTHER RESULTS, OF PROJECT TEL1998-1020

4.1 Design of a high security infrastructure for Internet.

The first and main achievement of the Module 1 has been the design, development and implementation of a **Public Key Infrastructure (PKI)** for the CSIC.

This CSIC-PKI allows to issue different classes of digital certificates for the staff, the servers and the certification authorities (CA) belonging to the CSIC. Also, the software objects developed for research groups of the CSIC. Thus, this service provide a mechanism to:

- secure the communications (email, SSL links)
- improve the access control to the resources
- protect the stored data
- certificate the origin and authenticity of the software design in the CSIC

CSIC-PKI is included in the certification authority pilot headed by RedIris and it has the hierarchical structure depicted in Figure 1. The elements included are:

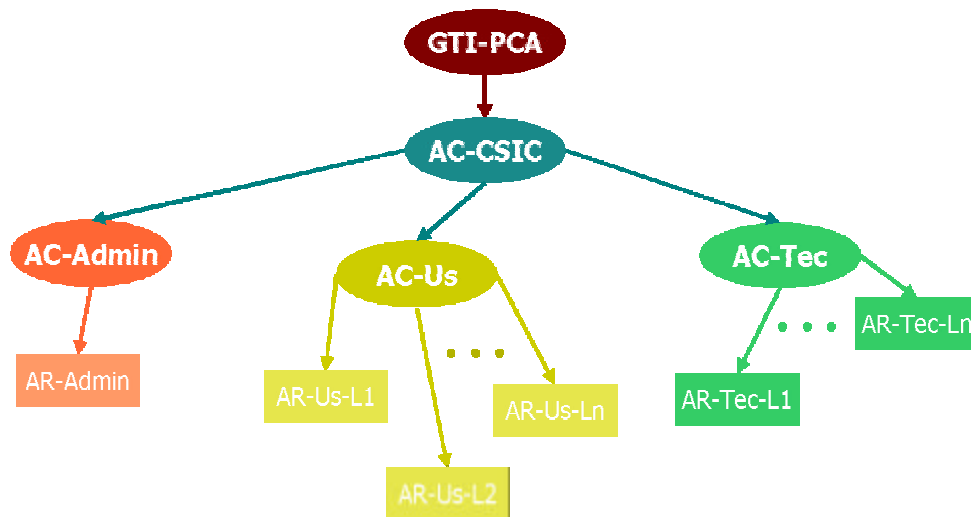


Figure 1.- Hierarchical Structure of CSIC-PKI

The elements included are:

- **GTI-PCA.-** RedIris Certification Authority
- **AC-CSIC.- (OID: 1.3.6.1.4.1.7457.4.2.1.1).**- Leader Certification Authority in the CSIC. It is signed by GTI-PCA and issues keys and certifications to institutional CAs only.
- **AC-Admin.- (OID: 1.3.6.1.4.1.7457.4.2.1.2).**- Institutional CA, it issues keys and certifications to Administrative Staff: Higher level Staff, Central Administration Staff, Directors and Managers of the CSIC Centres.
- **AC-Tec.- (OID: 1.3.6.1.4.1.7457.4.2.1.3).**- Secondary Institutional CA, certification issuer for technical subjects: technical staff, servers, other CAs, and objects.
- **AC-Us.- (OID: 1.3.6.1.4.1.7457.4.2.1.4).**- Secondary Institutional CA, personal certification issuer.

- **RA-Admin, RA-Tec, and RA-U.S.-** They are the registration authorities (RA) related to the institutional CAs.
- **Certification Policies.-** Documents describing a set of rules that indicates the applicability of a certificate issued by the CAs belonging to CSIC-PKI.
 - Política de certificación de AC-CSIC (OID: 1.3.6.1.4.1.7457.4.2.2.1.1.0)
 - Política de certificación de AC-Admin (OID: 1.3.6.1.4.1.7457.4.2.2.2.1.0)
 - Política de certificación de AC-Tec (OID: 1.3.6.1.4.1.7457.4.2.2.3.1.0)
 - Política de certificación de AC-U.S (OID: 1.3.6.1.4.1.7457.4.2.2.4.1.0)

Several schemes for CSIC-PKI were designed and evaluated but the present one was selected due to its adaptation to the complex structure of the CSIC. It is a modular and easily extensible to the geographical and administrative distribution of the CSIC. The information of the CSIC-PKI can be found in <http://acer.csic.es>.

The utilized OID's have been assigned by the CTI-CSIC, that has the branch OID 1.3.6.1.4.1.7457.1.4 assigned by RedIris.

The OID's specified in this project are composed by the following parts:

- 1 - ISO assigned OIDs.
- 1.3 - ISO Identified Organization.
- 1.3.6 - US Department of Defense.
- 1.3.6.1 - OID assignments from 1.3.6.1 - Internet.
- 1.3.6.1.4 - Internet Private.
- 1.3.6.1.4.1 - IANA-registered Private Enterprises.
- 1.3.6.1.4.1.7457 - Centro de Comunicaciones CSIC/RedIris.
- 1.3.6.1.4.1.7457.1 - Rama asignada por Centro de Comunicaciones CSIC/RedIris a centros asociados a RedIris.
- 1.3.6.1.4.1.7457.1.4 - CSIC-CTI
- 1.3.6.1.4.1.7457.1.4.1 - Centro Técnico de Informática
- 1.3.6.1.4.1.7457.1.4.2 - Objetos relacionados con PKI-X.509
- 1.3.6.1.4.1.7457.1.4.2.1 - Objetos relacionado con Identidades Digitales
- 1.3.6.1.4.1.7457.1.4.2.2 - Políticas de Certificación

More information about these OID's can be found in <http://www.cti.csic.es/OIDs>

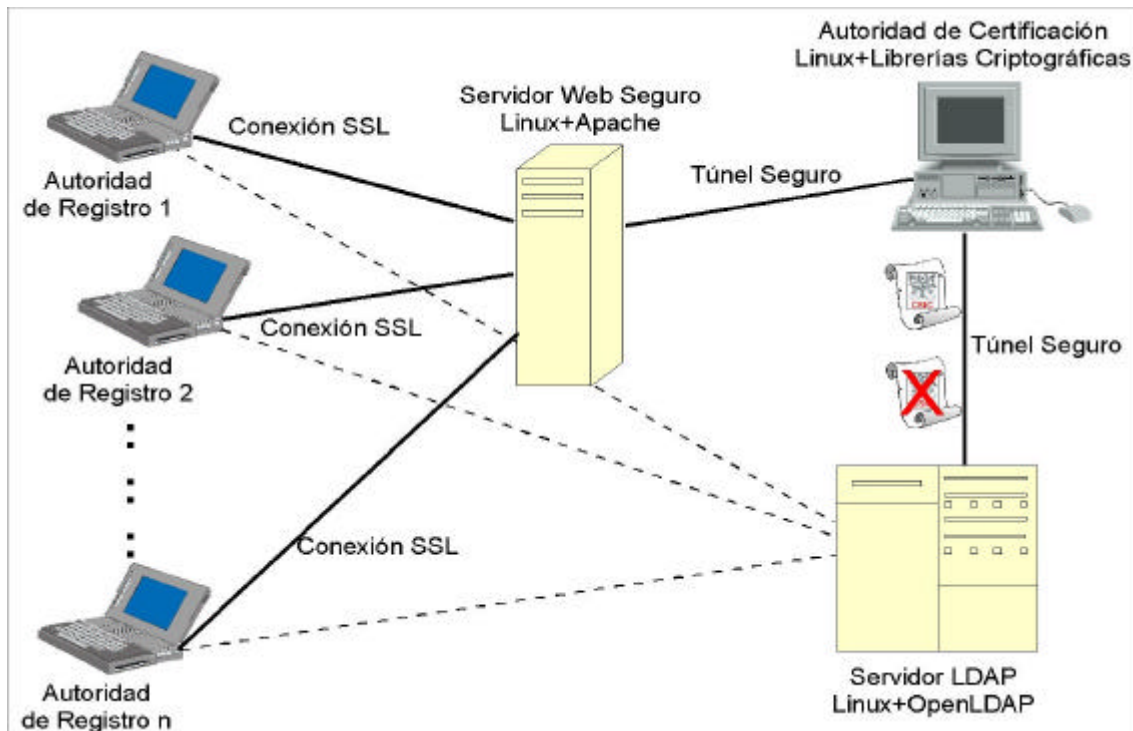


Figure 2.- CSIC Public Key Infrastructure scheme.

The results of this module have been transferred to CTI-CSIC (EPO of this project) and responsible of the CSIC-PKI management. The CSIC-PKI will be started at the beginning of year 2002.

The second achievement has been the development of a CryptoASP to add cryptographic strength to any web page based application, compatible with ActiveX.

ASP pages are created using scripting languages such as VBScript or JScript. These languages have the intrinsic limitation of lacking cryptographic functions to encrypt/decrypt text, hash documents or generate random numbers. This limitation can be overcome by the creation of a custom DLL incorporating all those cryptographic functions.

CryptoASP is an example of an ActiveX DLL which adds cryptographic strength to any web based application. It includes the following functions:

Encrypt: it takes as arguments a first string, representing the passphrase, and a second string, representing the plain text to be encrypted. By default, it uses RC4 stream cipher, although the algorithm to be used can be configured.

Decrypt: it takes as arguments a first string, representing the passphrase, and a second string, representing the cipher text to be decrypted. By default, it uses RC4 stream cipher, although the algorithm to be used can be configured. Obviously, it must be the same as the algorithm used in the encryption stage.

Hash: it takes as argument a string, representing the data whose hash must be calculated. The algorithm used is MD5, although it can be configured.

GenRandom: it takes as argument an integer number and returns a pseudo random number of length in bytes equal to the first argument.

As any DLL, it can be called from a script in a web page using ASP, or from any other application compatible with ActiveX. These four functions are implemented as calls to the CryptoAPI. Depending on the Cryptographic Service Providers (CSP) installed in the hosting machine, a different range of algorithms with variable key length will be used.

4.2 Design of a secret-key cryptosystems based on unidimensional cellular automata.

A *Unidimensional Cellular Automata* (CA) is a line of sites, called cells, with each site carrying the value $x_i \in GF(2)$. The cell values evolve synchronously in discrete time steps according to the values of other neighbour cells following a function or rule Φ . Although several authors have forecasted good prospects for the use of CA in Cryptography, our experience points to the opposite direction. From the very moment we started studying running-key generators based on CA, a clear conclusion was reached: Cellular Automata are not adequate structures to generate running-key sequences. In fact, the binary sequences obtained from the CA are defined by the following characteristics:

- Poor Statistics appreciated in such sequences (no balancedness, non-uniform distribution of 0's and 1's along the sequence, computation of wrong number of 0's and 1's runs ...)
- Low values of their linear complexity
- Short periods
- Unsatisfactory results in correlation tests

Never the less, there is a possible way of application of CA in Cryptography that we are considering presently. It can be summarised as follows:

The shrinking generator (SG) is a running-key generator made up of two different Linear Feedback Shift Registers (LFSR1 and LFSR2). The output sequence of such generator is a decimation of the output sequence of the LFSR1 according to the digits of the LFSR2 output sequence. That is to say, the SG output sequence is an irregular decimation of a PN-sequence.

Until now, we have realized that for specific LFSRs' lengths and feedback polynomials, the SG output sequence coincides with the sequence generated from a CA. More precisely, it coincides

with the CA corresponding to rule 90 (that is, the content of a cell at time t is the exclusive-OR of the contents of the two adjacent cells at time $t - 1$). This fact allows us to move from a non-linear structure such as the irregular decimation of a PN-sequence to a linear structure such as a CA with a particular rule.

At the moment our work is centered on two different goals:

Definition of the correspondence SG – CA for any couple of LFSRs in the shrinking generator.

Cryptanalysis of the shrinking generator in terms of its equivalent cellular automata.

Due to the non-satisfactory results obtained from the CA, we focussed our attention on another more conventional class of running-key generators such as the *non-linear filters* applied to LFSRs. That is the subject of the sections 1 and 2 in this report as previously explained (2.3).

Section 1:

This section includes a theoretical study on non-linear filters considered as running-key generators. The emphasis is on cryptographic properties of these generators such as period and linear complexity of their output sequences.

Among important results we can enumerate:

A mathematical modelling of non-linear filters, the so-called *Sequential Decomposition in Cosets*, that allows us to study easily the period and linear complexity of the obtained sequences.

Computation of the number of non-linear filters applied to any L -stage LFSR producing sequences with maximum period and linear complexity. The final result of this computation is that the probability of choosing a non-linear filter whose sequences have maximum period and linear complexity is $P = 0.997$ for LFSR of length 127.

A practical method to design non-linear filters whose output sequences have period and linear complexity adequate for their cryptographic application in secret-key cryptosystems.

A geometric interpretation of the linear complexity for binary running-key generators of low order.

RESULTS:

Software: There is not a great deal of software production as the majority of the results have been exclusively theoretical. Nevertheless, several programmes have been written (in C++) in order to check the numerical values provided by the above mentioned results.

Publications: [G-VF99], [FG-V99], [FC99], [FUS99], [FC00], [G-VF00], [FG-V01], [FG-V00a], [G-VF99a], [G-VF99b], [G-VF99c], [G-VF99d].

Doctoral Thesis: *Cotas de complejidad lineal para criptosistemas seguros en comunicaciones de banda ancha.*

Student: Luis Javier García Villalba.

University: Universidad Politécnica de Madrid.

Faculty: Dpto. de Lenguajes y Sistemas Informáticos e Ingeniería del Software. Facultad de Informática.

Year: June, 1999.

Grade: Sobresaliente CUM LAUDE.

Section 2:

It is a well known fact that a binary sequence of cryptographic application must be balanced. Roughly speaking, a binary sequence is balanced whether it has approximately the same number of 1's and 0's. Due to the long period of a cryptographic sequence (about 10^{50}), it is unfeasible to produce an entire cycle of such a sequence and count the number of 1's and 0's. Therefore, in practice, portions of the output sequence are chosen randomly and the frequent test (monobit test) is applied to all these subsequences. If all of them pass the statistical test, then the generator is accepted as "*being balanced*". Nevertheless, passing the frequency test merely provides probabilistic evidence that the generator produces a balanced sequence.

The problem we dealt with can be tackled as follows:

Given a generating function of a LFSR-based generator, we go to compute the number of 1's and 0's in the generated sequence. This computation is based exclusively on the particular form of the generating function.

In this way, the balancedness of the sequence can be easily determined. If the sequence were not balanced in a strict sense, then the degree of deviation from the theoretical value could always be derived. The algorithm that carries out this computation was first developed for non-linear filters (only one LFSR). Later, a generalisation of this result was applied to combination generators (more than one LFSRs). At the same time and as a straight consequence of this algorithm, two additional results were obtained:

An easy design strategy to generate guaranteed balanced sequences.

A method of boolean function conversion from Algebraic Normal Form (A.N.F.) into minterm representation.

RESULTS:

Software: A programme written in C++ that implements such an algorithm.

INPUT: The particular form of the non-linear generating function

OUTPUT: The precise number of 1's and 0's in the obtained sequence.

The execution time of this algorithm depends on the function form and the number of terms, ranging in the interval [a couple of hours – 2.5 days] for the cases we have considered. The programme ran on a PC (Pentium III , 800 MHz with 256 Mb of RAM).

Publications: [G-MF00], [G-MFG01], [FUS02], [FG-M01] In addition two different articles have been submitted to two specialized Journals.

Section 3:

In this section an algebraic cryptanalysis of the A5/2 algorithm for data protection in the GSM mobile communication system is described. Due to different weaknesses of this system concerning frequent re-initialisation, bad distribution of the feedback taps of the LFSRs as well as small number of skipped bits during the re-initialisation process, the output bits of this generator can be reconstructed in a rather efficient way. The attack is essentially one method of reconstructing such linear relations.

The cryptanalytic method can be summarized as follows:

A system of 64 non-linear equations of second order in 64 unknowns (the initial contents of the LFSRs) is first written. Later, the system is linearized giving rise to 719 equations with the same number of unknowns. When we tried to solve such a system of linear equations, we found that due to the weaknesses above mentioned we could not get 719 equations linearly independent. At most we got about 680, the rest were just linear combinations of the previous ones. Consequently, given a set of known output bits in the range of the number of linearly independent equations, we could deduce the majority of the resulting sequence as a linear combination of the known bits. The bits non-reconstructed correspond to degenerate cases including *pivoting*. At each clock pulse of the generator, a new equation is added to the system and its rank is checked. If the rank is not increased and the pivoting case does not take place, the corresponding unknown bit of the output sequence is calculated easily. The degenerate cases are not frequent. In any case, since the algorithm A5/2 is used for encryption of speech, the understandability of the reconstructed signal is not radically affected by the loss of a short run of degenerate bits.

In order to carry out this reconstruction, only 4 frames of known bits, not necessarily separated by a fixed distance, are required. Unlike other cryptanalytic methods found in the literature, this algorithm always finds the solution. The time complexity of the attack is 2^{17} . A process of precomputation enables this cryptanalytic algorithm to find the solution much faster. If the solution space is divided into independent parts associated with independent computers in a rather small network, then the solution can be found in real time. The method is also applicable to the cryptanalysis of similar schemes.

The implementation of this algorithm runs on a PC (Pentium III , 800 MHz with 256 Mb of RAM). For the same secret key given in <http://cryptome.org/gsm-a512.htm>, 1999, the program spent 2.5

hours to find the solution.

RESULTS:

Software: A programme written in Pascal that implements such an algorithm.

Publications: [PF00], [PF02],

Section 4:

This section deals with the application of the edit-distance technique to Cryptanalysis.

The edit-distance measure is defined as the minimum number of elementary edit-operations (deletions and substitutions) needed to transform a sequence **X** into a sequence **Y**. Restrictions on the length of the deletions and/or substitutions runs are also permitted.

The edit-distance technique can be applied to the cryptanalysis of running-key generators based on LFSRs whose decimated output sequences are the inputs to the non-linear generating function. In practice, the decimation devices are also LFSRs. The running-key sequence is currently modelled as an additive noise on the output generator sequence.

In edit-distance terms, a deletion can be interpreted as the decimation of a bit in the output LFSR sequence as well as a substitution can be interpreted as the addition of a noisy bit. Consequently, given the output sequence from a LFSR with a particular initial state before decimation (sequence **X**) and the output sequence from the generator after the addition of the noise (sequence **Y**) the edit-distance technique can be applied as follows:

Step 1: Compute the edit-distance between sequences **X** and **Y**. If this value is under a pre-defined threshold, then the LFSR initial state is accepted as solution candidate. Otherwise such an initial state is rejected.

Step 2: For every candidate state, reconstruct its corresponding decimation sequence and generate the final output sequence.

Step 3: Such an output sequence is compared with the intercepted running-key sequence (Hamming distance). If the number of coincidences is within a tolerance range, then that particular initial state is accepted as solution to the problem. Otherwise, take a new candidate state and goes to step 2.

The attack is effective and the solution to the cryptanalytic problem (that is to say the determination of the LFSR initial states) can be found. The performance of this technique is clearly limited by the lengths of the LFSRs involved in the generating scheme.

RESULTS:

Software: A program written in C++ that implements such an algorithm.

Publications:

[PFD01]

In this moment, there is in preparation an article to be submitted to a specialized Journal.

The stay of Dr Slobodan Petrovic in our Department for one year (April 2000 – April 2001) has been the first contact with the Department of Cryptography Faculty of Electrical Engineering of the University of Belgrade (Yugoslavia) considered as a leader group in the field of Cryptanalysis of secret-key cryptosystems. We keep a close relationship to the members of this cryptographic team in particular to Dr Jovan Golic and Dr Miodrag Mihaljevic.

REFERENCES

INTERNATIONAL PUBLICATIONS

- [AFG99] E. Álvarez, A. Fernández, P. García, J. Jiménez, A. Marcano, *New approach to chaotic encryption*, Phys. Lett. A, **263** (1999) 373-375.
- [AMR00c] G. Álvarez, F. Montoya, M. Romera y G. Pastor. *Cryptanalysis of a chaotic encryption system*, Physics Letters A, **276** (2000) 191-196.
- [BA00] K. M. Briggs, G. Alvarez, *Scaling in a map of the two-torus*, Experimental Mathematics, **9**(2) (2000) 301-307.
- [FC00] A. Fúster, P. Caballero. *Bitwise Operation Algorithm to Lower bound some Sequences Span*. International Journal of Applied Mathematics, **2** (5) (2000) 585-596.
- [FG-V01] A. Fúster, L. J. García Villalba. *An Efficient Algorithm to Generate Binary Sequences for Cryptographic Purposes*. Theoretical Computer Science. **259** (2001) 679-688
- [FUS02] A. Fúster. *Practical design of balanced sequence LFSR-based generators*. International Mathematical Journal. **1** (4), (2002) 349-361.
- [G-VF00] L. J. García-Villalba, A. Fúster. *On the Linear Complexity of the Sequences Generated by Nonlinear Filterings*. Information Processing Letters, **76** (2000) 67-73.
- [G-VF99] J. L. García-Villalba, A. Fúster. *On the General Classification of Nonlinear Filters of m -Sequences*. Information Processing Letters. **69** (1999) 227-232.
- [MMP99] F. Montoya Vitini, J. Muñoz Masqué, A. Peinado Domínguez. *Linear complexity of the $x^2 \bmod p$ orbits*. Information Processing Letters, **72** (1999) 3-7.
- [PF00] S. Petrovic, A. Fúster. *Cryptanalysis of the A5/2 Algorithm*. Cryptology ePrint Archive, International Association for Cryptological Research, Report 2000/052, <http://eprint.acr.org>, 2000.
- [PMM01] A. Peinado Domínguez F. Montoya Vitini J. Muñoz Masqué,. *Iterated Quadratic Functions in F_2^n* , International Journal of Applied Mathematics, **5** (1) (2001) 65-83.
- [PMMY01] A. Peinado, F. Montoya, J. Muñoz, A. J. Yuste, *Maximal Periods of x^2+c in F_q* , Lecture Notes in Computer Science, (2001), to appear.
- [PRAM01] G. Pastor, M. Romera, G. Álvarez and F. Montoya. *Misiurewicz point patterns generation in one-dimensional quadratic maps*, Physica A, **292** (2001) 207-230.
- [PRAM01a] G. Pastor, M. Romera, G. Álvarez and F. Montoya. *Operating with external arguments in the Mandelbrot set antenna*. Submitted to Physica D
- [PRAM01b] G. Pastor, M. Romera, G. Álvarez and F. Montoya. *Shrubs in Mandelbrot set ordering*. Submitted to Physica D
- [RBPAM00] M. Romera, V. Bañuls, G. Pastor, G. Álvarez and F. Montoya. *Snail-like pattern generation with the Hénon family of maps*. Computers and Graphics **25** (2001) 529-537
- [RPAM00] M. Romera, G. Pastor, G. Álvarez, F. Montoya. *Growth in complex exponential dynamics*. Computers & Graphics, **24** (2000) 115-131.
- [CM00] M. Castrillón López, L. Hernández Encinas, J. Muñoz Masqué, *Gauge invariance on interaction $U(1)$ bundles*, J. Physics A: Math. Gen. **33** (2000) 3253-3267.
- [CM99] M. Castrillón López, J. Muñoz Masqué. *Gauge forms on $SU(2)$ -bundles*, J. Geom. Phys. **30** (1999), 313-330.
- [CM99a] M. Castrillón López, J. Muñoz Masqué. *Gauge-invariant variationally trivial problems on T^*M* , J. Math. Phys. **40**, nº 2 (1999), 821-829.
- [CM99b] M. Castrillón López, J. Muñoz Masqué. *Structure symplectique généralisée sur le*

fibré des connexions, C.R. Acad. Sci. Paris **328**, Série I (1999), 41-44.

- [CMM99] M. Castrillón López, P. Martínez Gadea, J. Muñoz Masqué. *Distributions Admitting a Local Basis of Homogeneous Polynomials*, Libertas Math. **XIX** (1999), 19-27.
- [DM00] R. Durán Díaz, J. Muñoz Masqué, *Second-order Lagrangians admitting a second-order Hamilton-s A: Math. Gen.* **33** (2000) 6003-6016.
- [FGM00] Antonio Fernández, Pedro L. García, J. Muñoz Masqué, *Gauge-invariant covariant Hamiltonians*, J. Math. Phys. **41** (8) (2000) 5292-5303.
- [GMM00] Pedro M. Gadea, A. Montesinos Amilibia, Jaime Muñoz Masqué, *Characterizing the complex hyperbolic space by Kähler homogeneous structures*, Math. Proc. Cambridge Philos. Soc. **128** (2000) 87-94.
- [GRM99] L. J. Garcia-Villalba, M. C. Rodriguez-Palauquex and F. Montoya-Vitini. *Algorithm for computing minimum distance*. Electronics Letters, **35** (1999) 1534-1535
- [MM00] Agustín Marcelo, J. Muñoz Masqué, *Projective dimension in UFDs*, J. Pure Appl. Algebra **150** (2000) 301-306.
- [MP00] J. Muñoz Masqué, L. M. Pozo Coronado, *Parameter Invariance in Field Theory and the Hamiltonian Formalism*, Fortschr. Phys. **48** (4) (2000) 361-405.
- [MP99] J. Muñoz Masqué, L. M. Pozo Coronado. *Unrolling and rolling of curves in non-convex surfaces*, Inverse Problems **15**, nº 4 (1999), 869-880.
- [MS00] J. Muñoz Masqué, O. A. Sánchez Valenzuela, *Natural quotients on split supercotangent bundles and their canonical supersymplectic structures*, Differential Geom. Appl. **12** (2000) 85-103.
- [MV99] J. Muñoz Masqué, A. Valdés. *Characterizing the Blaschke connection*, Differential Geom. Appl. **11** (1999) 237-243.
- [CHH01] J. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández and M. Rodríguez Sánchez, *Designing hypermedia tools for solving problems in Mathematics*, Computers and Education, 2001 (por aparecer).

NATIONAL PUBLICATIONS

- [AC01] G. Álvarez y L. Cornide, *Anatomía de un ataque hacker*, iWorld, **39**, 55-64, junio 2001.
- [ALV00b] G. Álvarez. *Cómo restringir el acceso a páginas web*, iWorld, **23** (2000) 36-43.
- [ALV00c] G. Álvarez, *Internet Guard Dog*, PC World, **168**, 142-143, septiembre 2000.
- [ALV00o] G. Álvarez, *Rijndael, el nuevo estándar de cifrado*, SIC, **42**, 58, noviembre 2000.
- [ALV00d] G. Álvarez, *Cortafuegos: la mejor defensa*, iWorld, **31**, 68-76, octubre 2000.
- [ALV00e] G. Álvarez, *Servidores seguros*, PC World, **164**, 274-299, abril 2000.
- [ALV00f] G. Álvarez, *Algoritmo Rijndael: el estándar de cifrado del siglo XXI*, PC World, **170**, 20, noviembre 2000.
- [ALV00g] G. Álvarez, *Cómo sacarle todo el jugo al correo electrónico. Básico (I)*, iWorld, **31**, 90-91, octubre 2000.
- [ALV00h] G. Álvarez, *Cómo sacarle todo el jugo al correo electrónico. Intermedio (I)*, iWorld, **33**, 90-91, diciembre 2000.
- [ALV00i] G. Álvarez, *Las claves del correo electrónico*, PCWorld, **164**, 194-210, abril 2000.
- [ALV00j] G. Álvarez, *Correo Web: bueno, bonito y barato*, PCWorld, **167**, 230-243, julio/agosto 2000.
- [ALV00k] G. Álvarez, *De incógnito por Internet*, PC World, **168**, 144-178, septiembre 2000.
- [ALV00l] G. Álvarez, *Los secretos de la firma electrónica*, iWorld, **25**, 50-58, marzo 2000.
- [ALV00m] G. Álvarez. *La banca en casa: mercados bursátiles del nuevo siglo (y II)*, PC World,

162, (2000) 276-282

- [ALV00n] G. Álvarez, *Protección de derechos de autor en Internet*, *iWorld*, **30**, 60-68, septiembre 2000.
- [ALV01] G. Álvarez, *Acceso web a bases de datos*, *PCWorld*, **177**, 247-260, junio 2001.
- [ALV01a] G. Álvarez, *ActiveX: ¿Amigo o enemigo?*, *PC World*, **180**, 237-246, octubre 2001.
- [ALV01b] G. Álvarez, *Cómo sacarle todo el jugo al correo electrónico. Intermedio (y II)*, *iWorld*, **34**, 90-91, enero 2001.
- [ALV01c] G. Álvarez, *Cómo sacarle todo el jugo al correo electrónico. Avanzado (I)*, *iWorld*, **35**, 90-91, febrero 2001.
- [ALV01d] G. Álvarez, *Cómo sacarle todo el jugo al correo electrónico. Avanzado (II)*, *iWorld*, **36**, 90-91, marzo 2001.
- [ALV01e] G. Álvarez, *Las cookies al descubierto*, *PCWorld*, **172**, 242-253, enero 2001.
- [ALV99] G. Álvarez. *Cómo firmar applets de Java en cuatro pasos*, *PC World*, **155** (1999) 270-282
- [ALV99a] G. Álvarez. *Las reglas de oro para la navegación segura*, *PC World*, **153** (1999) 230-250
- [ALV99b] G. Álvarez. *Medios de pago en Internet: cómo comprar inteligentemente*, *PC World*, **156** (1999) 216-232
- [ALV99c] G. Álvarez. *Seguridad SSL*, *iWorld*, **18** (1999) 51-54
- [ALV99d] G. Álvarez. *Dinero electrónico*, *PC World*, **159** (1999) 324-342
- [ALV99e] G. Álvarez. *El banco en casa: banca digital (I)*, *PC World*, **161** (2000) 119-130
- [AMR00a] G. Álvarez, F. Montoya, M. Romera, G. Pastor. *Criptografía basado en la sincronización de osciladores caóticos*, *Mundo Electrónico* **307** (2000) 56-58.
- [AS99] G. Álvarez Marañón y Miguel A. F. Sanjuán. *Comunicaciones Seguras utilizando Señales Caóticas*, *Revista Española de Física* **13** (5), 23-27, 1999.
- [CRPAM01] J. Calvo, M. Romera, G. Pastor, G. Álvarez y F. Montoya, *Argumentos externos del conjunto de Mandelbrot*, *Revista Española de Física* **15** (3), (2001) 29-33
- [DHM00] R. Durán Díaz, L. Hernández Encinas, J. Muñoz Masqué, *Ataques a DES y módulos factorizados de RSA*, *SIC* **40** (2000), Ágora I-IV.
- [FG-V00a] A. Fúster, L. J. García Villalba. *Sobre el parámetro complejidad lineal y los filtros no lineales de segundo orden*. *Revista Matemática de la Universidad Complutense de Madrid* **13** (2000) 119-134
- [PEI99] A. Peinado. *Autoridades de Certificación I: Elementos esenciales en las comunicaciones seguras*, *BIT*, **114** (1999), 54-56
- [PEI99a] A. Peinado, *Autoridades de Certificación II: Aplicación al correo electrónico*, *BIT*, **115** (1999), 68-69
- [ALV00p] G. Álvarez. *Spam: el correo basura*, *ReD*, **27** (2000)
- [ALV00q] G. Álvarez. *WAP: Internet más móvil que nunca*, *iWorld*, **23** (2000) 44-51
- [ALV01f] G. Álvarez, *Dominando las hojas de estilo: CSS bajo control (I)*, *iWorld*, **38**, 88-91, mayo 2001.
- [ALV99f] G. Álvarez, *Dominando las hojas de estilo: CSS bajo control (y II)*, *iWorld*, **39**, 88-91, junio 2001. G. Álvarez. *ITS*, *iWorld*, **20** (1999) 64-70
- [ALV99g] G. Álvarez. *SET a fondo*, *iWorld*, **22** (1999) 64-70
- [HM99] L. Hernández Encinas y J. Minguet Melián, *Criptografía visual*, *Novática* **138** (1999), 63-68.

- [HER00] L. Hernández Encinas. *Taller de Criptomatemáticas para jóvenes (y adultos)*, SUMA **33** (2000), 45-58.
- [HMM00] Luis Hernández Encinas, Fausto Montoya Vitini y Jaime Muñoz Masqué. *Esquemas criptográficos visuales*. SIC **38** (2000) Agora IV-X.

CONFERENCE COMMUNICATIONS

- [ALV00] G. Álvarez, "Acceso seguro a páginas web", Mundo Internet 2000, 275-284, Madrid, febrero 2000.
- [ALV00a] G. Álvarez, "Programación en JavaScript", Mundo Internet 2000, 265-274, Madrid, febrero 2000.
- [AMO01] G. Álvarez, F. Montoya, A. Orúe. *On the security of Quantum Key Distribution protocols*, 5th World Multiconference on Systemics, Cybernetics and Informatics, SCI 2001 Proceedings, International Institute of Informatics and Systemics. Orlando (2001) ISBN 980-07-6702-9, pag 486-491
- [AMP 99] G. Álvarez, F. Montoya, G. Pastor, M. Romera, *Chaotic Cryptosystems*, IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology, 332-338, Madrid (1999).
- [AMRP 00] G. Álvarez, F. Montoya, M. Romera, G. Pastor. *Cryptanalytic methods in chaotic cryptosystems*, 5th World Multiconference on Systemics, Cybernetics and Informatics, SCI 2001 Proceedings, International Institute of Informatics and Systemics. Orlando (2000) ISBN 980-07-6702-9, pag 480-485
- [AMRP00] G. Álvarez, F. Montoya, M. Romera, G. Pastor. *Criptoanálisis de sistema caótico basado en la ergodicidad*, Criptología y Seguridad en la Información, P. Caballero Gil y C. Hernández Goya, eds. RA-MA, Madrid (2000) 437-447, ISBN 84-7897-431-8
- [CA01] L. Cornide y G. Álvarez, *CryptoBench: Un banco de pruebas para componentes criptográficos*, URSI 2001, Madrid, 2001.
- [DMM99] R. Durán Díaz, F. Montoya Vitini, J. Muñoz Masqué. *Densidad de primos seguros*, F.J. Ares Pena, E. Moreno Piquero y F. Obelleiro Basteiro, eds., Actas del XIV Simposium Nacional de la Unión Científica Internacional de Radio (URSI), Santiago de Compostela (Spain), September 8-10, 1999, Universidad de Santiago de Compostela (Spain), 1999, pp. 85-87. (ISBN: 84-699-0893-6)
- [DMM99a] R. Durán Díaz, F. Montoya Vitini, J. Muñoz Masqué. *Safe primes density and cryptographic applications*, Larry D. Sanson, ed., Proceedings of the 33rd Annual 1999 International Carnahan Conference on Security Technology, Madrid (Spain), October 5-7, 1999, The Institute of Electrical and Electronics Engineers, New York, NY, 1999, pp. 363-367. ISBN: 0-7803-5247-5
- [FC99] A. Fúster, P. Caballero. "An algorithm to compute the linear complexity of nonlinearly filtered sequences". Abstracts of the 8th International Colloquium on Numerical Analysis and Computer Science with Applications, pp. 68. Plovdiv, Bulgaria, 13-17 August 1999.
- [FG-M01] A. Fúster, P. García-Mochales. "Generadores binarios de secuencias equilibradas". Actas del XVI Simposium de la Unión Científica Internacional de Radio URSI'2001, pp. 237 - 238. Universidad Europea de Madrid, 19-21 Septiembre 2001.
- [FG-V99] A. Fúster, L.J. García-Villalba. "A Radix-Two Form Interpretation of the Linear Complexity of Non-linear Filters". Proceedings of the 5th International Symposium on Communication Theory and Application, ISCTA, pp. 225-227. Charlotte Mason College, Ambleside, UK, 11-16 July 1999.
- [FUS99] A. Fúster. "Non-linear filterings of m-sequences". International Meeting on Coding Theory and Cryptography, Medina del Campo (Valladolid), Spain, 6-8 September 1999.
- [FG-M01] A. Fúster, P. García-Mochales. *Generadores binarios de secuencias equilibradas*. Actas del XVI Simposium de la Unión Científica Internacional de Radio URSI'2001,

pp. 237 - 238. Universidad Europea de Madrid, 19-21 Septiembre 2001.

- [G-MF00] P. García-Mochales, A. Fúster. *Un algoritmo para calcular el número de ceros y unos en secuencias filtradas*. Actas de la VI Reunión Española sobre Criptología y Seguridad de la Información, pp. 307-317, Tenerife, 14-16 Septiembre de 2000. Editorial RA-MA. Madrid. (2000) ISBN-84-7897-431-8
- [G-MFG01] P. García_Mochales, A. Fúster, D. de la Guía. *Design of Balanced Sequences for Cryptographic Applications*. Proceedings of World Multiconference on Systemics, Cybernetics and Informatics, SCI 2001. vol. VII, pp. 500-504. Orlando, Florida, USA, 22-25 July 2001. ISBN-980-07-7547-1.
- [GP99] D. de la Guía Martínez, A. Peinado Domínguez. *Pseudorandom number generation based on Nongroup Cellular Automata*, Larry D. Sanson, ed., Proceedings of the 33rd Annual 1999 International Carnahan Conference on Security Technology, Madrid (Spain), October 5-7, 1999, The Institute of Electrical and Electronics Engineers, New York, NY, 1999, pp. 370-376. ISBN: 0-7803-5247-5
- [GUI00] de la Guía Martínez, Dolores. *Estado de las Autoridades de Certificación en España*. Jornadas Técnicas RedIris 2000 y Grupos de Trabajo, Murcia 13-17 de Noviembre de 2000.
- [GUI01] D. de la Guía Martínez. "Librerías Criptográficas". Jornadas Técnicas RedIris 2001 y Grupos de Trabajo, Pamplona, 22-26 de Octubre de 2001.
- [GP01] D. de la Guía, A. Peinado, *On the Sequences generated by 90-150 Programmable Cellular Automata*, Proc. of 5th World Multiconference on systemic, cybernetics and Informatics Vol. VII, Computer Science and Engineering. International Institute of Informatics and Systemics. Orlando, July 22-25, 2001, pp. 492-495. ISBN: 980-07-7547-1
- [G-VF99d] L. J. García-Villalba, A. Fúster. *Sobre una clasificación de los filtros no lineales de m-secuencias*. Actas del XIV Simposium de la Unión Científica Internacional de Radio URSI'99, pp. 92 - 93. Santiago de Compostela, 8-10 Septiembre 1999. ISBN-84-699-0893-6.
- [G-VF99a] L. J. García-Villalba, A. Fúster. *Generation of Binary Sequences for Cryptographic Applications*. Proceedings of the IEEE International Carnahan Conference on Security Technology, Madrid (Spain), October 5-7, 1999, The Institute of Electrical and Electronics Engineers, New York, NY, 1999, pp. 368-369. ISBN 0-7803-5247-5.
- [G-VF99b] L.J. García-Villalba, A. Fúster. *Pseudorandom Sequence Generators with Identical Cryptographic Properties*. International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT'99 (Rump Session). Prague, Czech Republic, May 2-6 1999. <http://www.iacr.org/conferences/ec99/rump.html>
- [G-VF99c] L.J. García-Villalba, A. Fúster. *Sequential Decomposition in Cosets of Non-linear Filtering of m-Sequences*. Actas de la Conferencia de Dispositivos Electrónicos CDE-99, pp. 535-538. Madrid 10-11 Junio 1999.
- [HER99] L. Hernández Encinas, *Tests estadísticos para el reconocimiento de números pseudoaleatorios en Criptología*, Actas de las Segundas Jornadas de Estadística Aplicada, 22-27. Universidad de Salamanca. 1999. ISBN: 84-88895-55-0.
- [HM00] L. Hernández, J. Muñoz Masqué, *Iterated discrete exponentiation and its cryptographic applications*, Jong Kun Lee, Matjaz Juric, Agostino Bruzzone, Daniel Klovshy, and Masahiro Fujita, eds., Proceedings of the "World Multiconference on Systemics, Cybernetics and Informatics, SCI 2000", Orlando, Florida (USA), July 23-26, 2000, Volume VIII, Computer Science and Engineering: Part II, International Institute of Informatics and Systematics, 2000, pp. 261-265 ISBN 980-07-6694-4.
- [HM00a] L. Hernández, J. Muñoz Masqué, *Una revisión de los generadores pseudoaleatorios del tipo $x^A \pmod{N}$* , Pino Caballero Gil y Candelaria Hernández Goya, eds., Actas de la VI Reunión Española sobre Criptografía y Seguridad de la Información (VI RECSI), Tenerife, Islas Canarias (España), septiembre 14-16, 2000, RA-MA Editorial, Madrid, España, 2000, pp. 297-305, ISBN 84-7897-431-8.

- [HM01] L. Hernández Encinas and J. Muñoz Masqué, *The number of hyperelliptic curves over a finite field. Recent results*, Proceedings of The 5th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2001), Volume VII: Computer Science and Engineering, 505-510. International Institute of Informatics and Systemics (IIS), Orlando (FL., U.S.A.), 2001. ISBN: 980-07-7547-1.
- [MMP99a] F. Montoya Vitini, J. Muñoz Masqué, A. Peinado Domínguez. *Bound for Linear Complexity of Quadratic Functions in F_p* , Larry D. Sanson, ed., Proceedings of the 33rd Annual 1999 International Carnahan Conference on Security Technology, Madrid (Spain), October 5-7, 1999, The Institute of Electrical and Electronics Engineers, New York, NY, 1999, pp. 349-353. ISBN: 0-7803-5247-5
- [MP00] F. Montoya, A. Peinado, *On the linear complexity of iterated discrete square function*, Proc. of 4th World Multiconference on systemic, cybernetics and Informatics (SCI2000), Orlando, Florida, USA, July 23-26 (2000), pp. V-254-259.
- [MP01] L. Moraga, A. Peinado, *Esquema de Votación Electrónica en entorno universitario*, Actas de las III Jornadas de Ingeniería Telemática (JITEL'01), Sept. 2001.
- [PEI00] A. Peinado, *Internet: ¿un entretenimiento o una herramienta de trabajo?*, Aula de Formación Abierta 2.000, Universidad de Málaga, pp. 427-428 (2000), ISBN: 84-7496-817
- [PEI00a] A. Peinado, *Estudio de las secuencias binarias producidas por el generador cuadrático mod p* , VI Reunión Española de Criptología y Seguridad de la Información, Tenerife, 14-16 Septiembre (2000), 319-326
- [PEI00b] A. Peinado, *Iterated square functions in $GF(2^n)$ and their cryptographic applications*, Ninth International Colloquium on Numerical Analysis and Computer Science with Applications, Plovdiv, Bulgaria, August 12-17, (2000). 49
- [PET00] S. Petrovic, *Un ataque por correlación sobre un generador de secuencia con registro de desplazamiento y función con memoria*, Pino Caballero Gil y Candelaria Hernández Goya, eds., Actas de la VI Reunión Española sobre Criptografía y Seguridad de la Información (VI RECSI), Tenerife, Islas Canarias (España), septiembre 14-16, 2000, RA-MA Editorial, Madrid, España, 2000, pp. 455. ISBN 84-7897-431-8.
- [PF02] S. Petrovic, A. Fúster. *Criptoanálisis del algoritmo A5/2 para telefonía móvil*. Primer Congreso Iberoamericano de Seguridad Informática. Morelia (México) Febrero 2002. (Accepted).
- [PFD01] S. Petrovic, A. Fúster, R. Durán. *The Use of Edit-Distances in Cryptanalysis*. Proceedings of World Multiconference on Systemics, Cybernetics and Informatics, SCI 2001. vol. VII, pp. 511-516. Orlando, Florida, USA, 22-25 July 2001. ISBN-980-07-7547-1.
- [PM00] Alberto Peinado Domínguez and Fausto Montoya Vitini. *On the Linear Complexity of iterated discrete square function*, 4th World Multiconference on Systemics, Cybernetics and Informatics SCI 2000 Proceedings, International Institute of Informatics and Systemics. Orlando (2000) ISBN 980-07-6702-9
- [PMM99] A. Peinado, J. Muñoz, F. Montoya, *Bounds for Linear Complexity of Quadratic Functions in F_p* , Proceedings of the 33rd Annual 1999 International Carnahan Conference on Security Technology, Madrid (Spain), October 5-7, 1999, The Institute of Electrical and Electronics Engineers, New York, NY, (1999) 349-353. ISBN: 0-7803-5247-5
- [QH01] Queiruga Dios y L. Hernández Encinas, *Exponentes de cifrado pequeños en RSA y criptoanálisis de Wiener*, Actas del XVI Simposium Nacional de la Unión Científica Internacional de Radio, 225-226. Universidad Europea de Madrid. 2001.
- [DGMM00] R. Durán Díaz, P.M. Gadea, J. Muñoz Masqué, *Variedades de Stein paracomplejas*, Elisa Linares Fuster y Juan Monterde García, eds., Actas del "VII Encuentro de Otoño de Geometría Diferencial y sus Aplicaciones", Valencia (España), septiembre 21-23, 1998, Publicaciones de la Real Sociedad Matemática Española, Volumen 1, Real Sociedad Matemática Española, Madrid, España, 2000, pp. 57-70. ISBN 84-

923818-1-7.

- [MP00a] J. Muñoz Masqué, L.M. Pozo Coronado, *Hamiltonian Formulation and Order Reduction for Nonlinear Splines in the Euclidean 3-Space*, A.G. Nikitin and V.M. Boyko, eds., Proceedings of the Third International Conference on "Symmetry in Nonlinear Mathematical Physics", Kyiv (Ukraine), July 12-18, 1999, Part 1, Institute of Mathematics of the National Academy of Sciences of Ukraine, 2000, pp. 170-176 ISBN: 966-02-1444-8; ISBN for Part 1: 966-02-1401-4.
- [RM99] Martín del Rey, J. Muñoz Masqué, *The problem of lifting diffeomorphisms*, Gheorge Pitit and Gheorge Munteanu, eds., Proceedings of the "Fourth International Workshop on Differential Geometry", Brasov (Romania) September 16-22, 1999, Transilvania University Press, Brasov, Romania, 2000, pp. 163-166. ISBN 973-9474-68-3.
- [PEI01] A. Peinado, *Breve Historia de la Criptografía*, Aula de Formación Abierta **2.001**, Universidad de Málaga, pp. 321-325 (2001), ISBN: 84-7496-880-1
- [GP01a] C. García, A. Peinado, *Herramienta Software para el aprendizaje sobre marcas de agua digitales en señales de audio*, Actas del XVI simposium nacional de la Unión Científica Internacional de Radio (URSI'01).19-21 Sept. 2001
- [CHH01a] J. M. Chamoso Sánchez, L. Hernández Encinas, J. Martín Lalanda, R. López Fernández y M. Rodríguez Sánchez. "Un CD-ROM para la numeración". Por aparecer en *Actas de las X Jornadas sobre el Aprendizaje y Enseñanza de las Matemáticas*. Federación Española de Sociedades de Profesores de Matemáticas. Zaragoza, 2001.
- [CHH00] J. M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández y M. Rodríguez Sánchez, Editores de las Actas del 6º Seminario Castellano-Leonés de Educación Matemática, *Pitágoras interactivo*. Burgos 2000. Por aparecer.
- [CHH00a] J. M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández y M. Rodríguez Sánchez, *Los sistemas hipermedia, ¿un posible camino para enseñar Matemáticas?*, Actas del IV Simposio sobre propuestas metodológicas y de evaluación en la formación inicial de los profesores del área de Didáctica de las Matemáticas, 245-253. Universidad de Oviedo. Oviedo, 2000.
- [CHP01] M. Chica, A. Peinado, *Herramienta para el aprendizaje de técnicas espaciales para inserción/detección de marcas de agua en Imágenes*, Actas del XVI simposium nacional de la Unión Científica Internacional de Radio (URSI'01).19-21 Sept. 2001
- [RCHH99] M. Rodríguez Sánchez, J. M. Chamoso Sánchez, L. Hernández Encinas y R. López Fernández, *Resolución de problemas mediante un CD-ROM*, Actas de las IX Jornadas sobre el Aprendizaje y Enseñanza de las Matemáticas, 276-280. Federación Española de Sociedades de Profesores de Matemáticas. Lugo, 1999. ISBN: 84-920438-3-0.

BOOKS

Amparo Fúster, Dolores de la Guía, Luis Hernández, Fausto Montoya y Jaime Muñoz: *Técnicas Criptográficas de protección de datos*, 2ª Edición Actualizada. Editorial: RA-MA, Madrid, (2000). ISBN 84-7897-421-0

L. Hernández Encinas y J. Rubio Álvarez (eds.), *Actas del 5º Seminario Castellano-Leonés de Educación Matemática*. 297 pp. Zamora, 2000. ISBN: 84-922919-3-1.

L. Hernández Encinas, *Técnicas de Taxonomía Numérica*, Cuadernos de Estadística 18, Arco-La Muralla, 159 pp. Madrid, 2001. ISBN: 84-7133-715-0.

N. Callaos, B. Sánchez, L. Hernández Encinas and J. Grzymala Busse (eds.). *Proceedings of The 5th World Multiconference on Systemics, Cybernetics and Informatics, Volume VII: Computer Science and Engineering*. International Institute of Informatics and Systemics, 2001. ISBN: 980-07-7547-1.

N. Callaos, L. Hernández Encinas et al. (eds.), *Proceedings*, 5th World Multiconference on Systemics, Cybernetics and Informatics, CD-ROM, 2001. ISBN: 980-07-7529-3.

WEB PUBLICATIONS

Gonzalo Álvarez Marañón, Página web: <http://www.iec.csic.es/criptonomicon/>, sobre seguridad informática en Internet. Es la referencia obligada sobre seguridad en Internet en castellano.

CONFERENCE PROGRAM COMMITTEE MEMBER

L. Hernández Encinas, *The 5th World Multiconference on Systemics, Cybernetics and Informatics*. SCI 2001. Orlando, USA. Julio'2001

L. Hernández Encinas, *VI Reunión Española de Criptología y Seguridad de la Información (VI RECSI)*, Asociación Española de Criptología. Universidad de Tenerife. Tenerife. Septiembre'2000.

L. Hernández Encinas, *The 3rd International Conference/Workshop on Automatic Differentiation (AD2000): from Simulation to Optimization*. SIAM, INRIA and Université Nice Sophia Antipolis. Nice, France. Junio'2000.

Amparo Fúster Sabater, *VI Reunión Española sobre Criptografía y Seguridad de la Información*. Tenerife. Septiembre 2000.

CONFERENCE INVITED CHAIRMAN

L. Hernández Encinas, *Theoretical Methods in Criptology*, The 5th World Multiconference on Systemics, Cybernetics and Informatics. SCI 2001. Orlando, USA. Julio'2001.

LECTURES

Amparo Fúster Sabater. *Nonlinear filtering of m-sequences*. Participación en el Seminario: International Meeting on Coding Theory and Cryptography, Medina del Campo (Valladolid), Spain, 6-8 September 1999.

Amparo Fúster Sabater. *An Algorithm to Compute the Linear Complexity of Nonlinearly Filtered Sequences*. Invited Speaker at "The Eighth International Colloquium on Numerical Analysis and Computer Science with Applications", Plovdiv (Bulgaria). 13-17 August 1999

Conferencia "Internet: ¿un entretenimiento o una herramienta de trabajo?", Málaga, 23 de mayo de 2000. Paraninfo de la Universidad de Málaga. Programa Aula de Formación Abierta para Mayores de la Universidad de Málaga.

Conferencia "Notaría electrónica", IV Simposium Internacional de Sistemas Computacionales e Informática, 7-9 de noviembre de 2000, Instituto Tecnológico de Zacatecas, Zacatecas, Zac, México.

Conferencia "Seguridad en las Comunicaciones", IV Simposium Internacional de Sistemas Computacionales e Informática, 7-9 de noviembre de 2000, Instituto Tecnológico de Zacatecas, Zacatecas, Zac, México.

Conferencia "El Comercio Electrónico en la PYME", Jornada para la Difusión del proyecto REDCNL.COM, 15 de febrero de 2001, Cámara de Comercio, Málaga.

Conferencia "Breve Historia de la Criptografía", Málaga, 3 de abril de 2001. Paraninfo de la Universidad de Málaga. Programa Aula de Formación Abierta para Mayores de la Universidad de Málaga.

L. Hernández Encinas and J. Muñoz Masqué, *Invariants of hyperelliptic curves of genus 2 over finite fields*, Poster, Third European Congress of Mathematics. Barcelona, 2000.

J. M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández and M. Rodríguez Sánchez, *Multimedia resources for Mathematical Education*, Teaching of Information and Communication Sciences, Euroconference'99 (New Technologies for Higher Education), Universidad Pontificia de Salamanca, Universidade de Aveiro and TMR (Training and Mobility of Researchers). Salamanca, 1999.

PhD. THESES

Doctoral Thesis: *Contribución al estudio de la estructura interna del Conjunto de Mandelbrot y aplicaciones en Criptografía*

Student: Gonzalo Álvarez Marañón.

Directors: Fausto Montoya Vitini and Miguel Romera García.

University: Universidad Politécnica de Madrid.

Faculty: Facultad de Informática. Dpto. de Lenguajes y Sistemas Informáticos e Ingeniería del Software.

Year: September, 2000.

Grade: Sobresaliente CUM LAUDE.

Doctoral Thesis: *Análisis de una experiencia de resolución de problemas para la mejora de la enseñanza-aprendizaje de las Matemáticas*

Student: José M^a Chamoso Sánchez

Director: Luis Hernández Encinas

University: Salamanca..

Faculty: Facultad de educación. Dpto. Didáctica de las Matemáticas y de las Ciencias Experimentales

Year: November, 2000.

Grade: Sobresaliente CUM LAUDE.

Doctoral Thesis: *Cotas de complejidad lineal para criptosistemas seguros en comunicaciones de banda ancha.*

Student: Luis Javier García Villalba.

Director: Amparo Fúster Sabater.

University: Universidad Politécnica de Madrid.

Faculty: Facultad de Informática. Dpto. de Lenguajes y Sistemas Informáticos e Ingeniería del Software.

Year: June, 1999.

Grade: Sobresaliente CUM LAUDE.

GRADUATION THESES

Diseño e Implementación de un Esquema de Votación Electrónica en entorno universitario, L. Moraga, Ingeniería de Telecomunicación (2001)

Herramienta de Aprendizaje sobre marcas de agua digitales en imágenes, M. Chica, Ingeniería Técnica de Telecomunicación - Esp- Sonido e Imagen (2001)

Herramienta de Aprendizaje sobre marcas de agua digitales en audio, C. García, Ingeniería Técnica de Telecomunicación - Esp. Sonido e Imagen (2001)

Modelado en SDL del sistema de Comunicaciones Móviles UMTS (RLC), Ingeniería de Telecomunicación

Modelado en SDL de funciones avanzadas de sistemas de comunicaciones móviles de 3^a Generación, Ingeniería de Telecomunicación

Estudio de la generación de secuencias pseudoaleatorias para cifrado en Flujo, Ingeniería de Telecomunicación

Mercado digital de imágenes mediante técnicas de espectro ensanchado, Ingeniería Técnica de Telecomunicación - Esp- Sonido e Imagen

Aplicación de un modelo psicoacústico a las marcas de agua en señales de audio, Ingeniería Técnica de Telecomunicación - Esp. Sonido e Imagen

COURSES

Curso de formación para empresas de la Comunidad de Madrid: *Protección de la Información y Seguridad en Internet*

Organizado por la Universidad Politécnica de Madrid

Financiado por el Fondo Social Europeo y la Comunidad de Madrid

Lugar y fechas de celebración: Escuela Universitaria de Informática-UPM, Madrid, 18 de febrero - 14 de abril. 2000
Profesores: J. Ramió Aguirre, D. de la Guía Martínez, G. Bravo García
Duración: 100 horas

Curso: Nuevos Enfoques de Seguridad Informática,
Organiza: Iniciativas empresariales
Lugares y fechas de celebración: Barcelona, 13 de abril, y Madrid, 15 de abril. 2000
Profesores: J. Ramió Aguirre, D. de la Guía Martínez
Duración: 7 horas.

Gonzalo Álvarez, "Herramientas utilizadas en las iniciativas de comercio electrónico: su necesidad, uso y seguridad", dentro del curso "Comercio Electrónico: Seguridad y Economía en la Red", de la Universidad Internacional del Mar 2000, Cieza, julio 2000.

Curso de criptografía y seguridad en redes para la empresa Airtel, 3 abril - 14 abril de 2000.

Tipo: Curso organizado por la empresa Iniciativas Empresariales
Título: Nuevos Enfoques de Seguridad Informática
Lugar de celebración: Barcelona y Madrid.
Profesores del curso: Jorge Ramió Aguirre y Dolores de la Guía Martínez.
Ambito: Nacional
Fechas: Abril 1999 (1ª edición), Abril 2000 (2ª edición), Abril 2001 (3ª edición).
Duración: 7 horas

Tipo: Curso de Especialización
Título: Seguridad en Redes Informáticas
Lugar de celebración: Facultad de Ingeniería Eléctrica, Universidad de Oriente, Cuba.
Profesores del curso: Dolores de la Guía Martínez.
Ambito: Internacional
Fechas: Julio 1999
Duración: 40 horas

Tipo: Curso de formación para empresas de la Comunidad de Madrid
Título: Protección de la Información y Seguridad en Internet
Organizado por la Universidad Politécnica de Madrid
Financiado por el Fondo Social Europeo y la Comunidad de Madrid
Lugar de celebración: Escuela Universitaria de Informática-UPM, Madrid
Ambito: Comunidad Autónoma de Madrid
Fechas: 18 de febrero - 14 de abril. 2000
Profesores: J. Ramió Aguirre, D. de la Guía Martínez, G. Bravo García
Duración: 100 horas

Tipo: Curso de formación para personal del CSIC
Título: Seguridad en Unix
Organizado por el Gabinete de Formación del CSIC
Lugar de celebración: Centro Técnico de Informática - CSIC, Madrid
Ambito: CSIC
Fechas: 28 de mayo - 1 de junio, 2001
Profesores: A. Herrero Pertierra, J. M. Bolaños Ladrón de Guevara, J. Hierro Díaz, A. Chicharro Ruiz, D. de la Guía Martínez
Duración: 20 horas

PATENTS

Autores: Gonzalo Álvarez Marañón, Amparo Fúster Sabater, Dolores de la Guía Martínez, Fausto Montoya Vitini y Alberto Peinado Domínguez.
Título: Método y aparato para cifrado en bloque de datos.
Número de publicación: 2.123.443
Año: 1999, 16 de Septiembre.
País: España. Entidad titular: CSIC.

CONTRACTS

Empresa: VISA INTERNATIONAL, California, (USA)

Contrato : Security evaluation of the Common Electronic Purse Specification (CEPS).

Empresa: VISA INTERNATIONAL, California, (USA)

Contrato: Security evaluation of the version 2.1 of the "Common Electronic Purse Specifications", developed by CEPSCO

Empresa: AIRTEL MÓVIL, S.A.

Contrato: Curso de criptografía aplicado a telefonía GSM

Empresa: AIRTEL MÓVIL, S.A.

Contrato: Evaluación de la seguridad de los algoritmos de cifrado e identificación en telefonía GSM y recomendaciones para su mejora

COLLABORATION WITH OTHER RESEARCH GROUPS

- Prof. Alan Mackay, Birkbeck College, University of London, (UK).
- Dr. Wolf Jung, Institut für Reine und Angewandte Mathematik, RWTH Aachen, (Deutschland)
- Prof. Jovan Golic, Prof. Miodrag Mihaljevic, and Dr. Slobodan Petrovic, Department of Cryptography Faculty of Electrical Engineering of the University of Belgrade (Yugoslavia).
- Prof. Alfred Menezes from the Centre for Applied Cryptographic Research (CACR) in the University of Waterloo (Canada).
- Prof. Jeffrey Shallit, Dep. Of Mathematics, University of Waterloo (Canada).
- Prof. Amalia Orúe, Prof. Bertha Soriano and Prof. Enrique Castro, Faculty of Electrical Engineering, Universidad de Oriente, Santiago de Cuba, (Cuba).
- D. Miguel Ángel Fernández Sanjuán, PhD (UNED). Escuela Superior de Ciencias Experimentales e Ingeniería de la Universidad Rey Juan Carlos. Madrid, (España)
- Prof. Michael Peter Kennedy PhD(Calif) FIEEE. Department of Microelectronic Engineering University College Cork Lee Maltings. Cork, (Ireland).
- Dr. Keith M. Briggs. Complexity Research Group, BTexaCT Research. Martlesham Heath, Suffolk, (UK).
- Dr. Marius-F. Danca, Department of Mathematics, Spiru Haret College. Cluj-Napoca, (Romania).