



Conferenciantes Plenarios	Comité Científico	Comité Organizador
Miguel Escobedo Martínez Marco Antonio López Cerdá Francisco Santos Leal Xavier Tolsa Domènech Premios JLRdF Santiago Morales Domingo (2006) Pablo Mira Carrillo (2007)	J. L. Vázquez Suárez (Presidente) Santos González Jiménez Wenceslao González Manteiga Daniel Hernandez Ruipérez Marc Noy Serrano Ana Vargas Rey	Consuelo Martínez López (Presidenta) Pedro Alonso Velázquez Carmen Corral Zapico Ignacio Fernández Rúa M ^a Concepción Masa Noceda Pablo Pérez Riera



entidades colaboradoras

www.uniovi.es/rsme09/



Resúmenes del Congreso de la Real Sociedad Matemática Española

Oviedo, 4 a 7 de febrero de 2009

Sesión especial 13: Nuevos avances en Criptografía y Codificación de la Información

Índice

Horario de la sesión	1
Construcciones lexicográficas de palabras minimales en códigos binarios	3
Sobre algunos aspectos de la teoría de códigos combinatoria	4
Tendencias actuales en cifrado en flujo: The eSTREAM Project	5
Seguridad Matemática en Redes Ad-hoc Vehiculares	6
Códigos de evaluación definidos por valoraciones	7
Códigos algebraico-geométricos sin geometría algebraica	8
Criptografía con curvas elípticas	9
Criptografía con curvas hiperelípticas de género 2	10
Configuraciones Combinatóricas y Recuperación Privada de Información por Pares	11
Aspectos criptográficos de algunas secuencias pseudoaleatorias	12
Verificabilidad en Criptografía	13
Sobre algunas construcciones de funciones bent	14

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Horario de la sesión

MIÉRCOLES 4

16:00 – 16:30

E. Martínez-Moro, M. A. Borges-Trenard, M. Borges-Quintana: *Construcciones lexicográficas de palabras minimales en códigos binarios*

16:30 – 17:00

J. Rifà, J. Borges, M. Villanueva: *Sobre algunos aspectos de la teoría de códigos combinatoria*

17:00 – 17:30

A. Fúster Sabater, M. E. Pazo Robles: *Tendencias actuales en cifrado en flujo: The eSTREAM Project*

17:30 – 18:00

Pino Caballero Gil: *Seguridad Matemática en Redes Ad-hoc Vehiculares*

JUEVES 5

11:30 – 12:00

Carlos Galindo: *Códigos de evaluación definidos por valoraciones*

12:00 – 12:30

Carlos Munuera López: *Códigos algebraico-geométricos sin geometría algebraica*

12:30 – 13:00

Anna Rio: *Criptografía con curvas elípticas*

13:00 – 13:30

L. Hernández Encinas, J. Muñoz Masqué: *Criptografía con curvas hiperelípticas de género 2*

VIERNES 6

11:30 – 12:00

Maria Bras-Amorós, Josep Domingo-Ferrer, Klara Stokes: *Configuraciones Combinatóricas y Recuperación Privada de Información por Pares*

12:00 – 12:30

Domingo Gómez: *Aspectos criptográficos de algunas secuencias pseudoaleatorias*

12:30 – 13:00

Jorge L. Villar: *Verificabilidad en Criptografía*

13:00 – 13:30

Joan-Josep Climent, Francisco J. García, Verónica Requena: *Sobre algunas construcciones de funciones bent*

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Construcciones lexicográficas de palabras minimales en códigos binarios

E. Martínez-Moro¹, M. A. Borges-Trenard², M. Borges-Quintana²

The error-correction problem in coding theory addresses given a received word recovering the codeword closest to it in Hamming distance. The usual formulation of this problem is the *maximum likelihood decoding problem* (MLDP), i.e. for a code and a received word the goal is to find the nearest codeword. The MLDP was studied by Berlekamp et al. [1] and they showed that it is NP-hard. In the MLDP of linear codes there is some freedom in the choice of which errors will be corrected in the sense that the correctable errors are the coset leaders, and when there is more than one vector of minimum weight in a coset, any one of them can be selected as the coset leader. It is a known fact that if lexicographically smallest minimum-weight vectors are chosen as the coset leaders then the set of correctable errors is endowed with a monotone structure. We will show an algorithmic procedure to compute the additive structure of the (monotone) coset leaders related with reduction (MLDP) and with set of minimal codewords (see for example [2] and the references therein).

Keywords: Maximum Likelihood Decoding Problem, Minimum Weight Vectors

Mathematics Subject Classification 2000: 94B99

Referencias

- [1] E.R. BERLEKAMP, R.J. McELIECE, H.C.A. VAN TILBORG On the Inherent Intractability of Certain Coding Problems. *IEEE Transactions on Information Theory*, **Vol. IT-24**, n. 3, pp. 384–386, 1978.
- [2] M. BORGES-QUINTANA, M.A. BORGES-TRENARD, P. FITZPATRICK, , E. MARTÍNEZ-MORO On a Gröbner Bases and Combinatorics for Binary Codes. *Appl. Algebra Engrg. Comm. Comput.* **Vol. 19**, n. 5, pp. 393–411 (2008)

¹Departamento de Matemática Aplicada
Universidad de Valladolid, Campus de Soria
E-42003, Castilla, Soria, Spain
edgar@maf.uva.es
<http://www.singacom.uva.es/~edgar>

²Dpto. de Matemática
FCMC, Universidad de Oriente
Santiago de Cuba, Cuba
{mborges,mijail}@csd.uo.edu.cu

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Sobre algunos aspectos de la teoría de códigos combinatoria

J. Rifà¹, J. Borges¹, M. Villanueva¹

En esta comunicación presentamos algunos aspectos de la teoría de la codificación en su vertiente combinatoria.

Describimos los códigos completamente regulares junto con resultados relacionados con problemas de no existencia y, también, con construcciones de nuevos códigos de esta familia.

Una clase importante de códigos completamente regulares son los códigos perfectos que son aquellos para los cuales el radio de recubrimiento iguala la capacidad correctora. La clasificación de los códigos 1-perfectos parece, actualmente, lejos de conseguirse y se utilizan algunos invariantes para ayudar en esta posible clasificación. Repasaremos alguno de estos invariantes, como por ejemplo el rango y la dimensión del núcleo y daremos algunos resultados en esta dirección.

Estudiaremos algunos códigos no lineales, pero con alguna estructura algebraica subyacente y, concretamente, daremos una breve introducción a los códigos llamados $\mathbb{Z}_2\mathbb{Z}_4$ -lineales, sus parámetros, matriz generadora, dualidad, etc.

Finalmente, algunos códigos combinatorios, como los códigos de Hadamard y los códigos 1-perfectos (extendidos o no) serán utilizados para estudiar intersecciones entre códigos isomorfos entre sí y calcular el cardinal de estas intersecciones, así como la estructura algebraica de las mismas.

Keywords: teoría de la codificación, combinatoria, códigos completamente regulares, códigos perfectos, $\mathbb{Z}_2\mathbb{Z}_4$ -linear code

Mathematics Subject Classification 2000: 94B25, 94B60, 05E30

Referencias

- [BRZ08] J. BORGES, J. RIFÀ, V.A. ZINOVIEV, On non-antipodal binary completely regular codes, *Discrete Mathematics*, **308**(16), 3508–3525, 2008.
- [RSV07] J. RIFÀ, F. I. SOLOV'ÉVA, M. VILLANUEVA, On the intersection of $\mathbb{Z}_2\mathbb{Z}_4$ -additive perfect codes, *IEEE Trans. Inform. Theory*, **54**(3), 1346–1356, 2008.

¹Departamento de Ingeniería de la Información y de las Comunicaciones
Universidad Autònoma de Barcelona
Campus Bellaterra, 08193 - Cerdanyola del Vallès
{josep.rifa, joaquim.borges, merce.villanueva}@uab.cat

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Tendencias actuales en cifrado en flujo: The eSTREAM Project^{*}

A. Fúster Sabater¹, M. E. Pazo Robles²,

El Proyecto eSTREAM para la selección de algoritmos de cifrado en flujo orientados al software ó al hardware ha modificado los planteamientos tradicionales de este tipo de criptosistemas. En este trabajo se describe el desarrollo de dicho proyecto y las consecuencias que, a corto y medio plazo, tendrá sobre la criptografía de clave secreta.

Keywords: Cifrado en fujo, eSTREAM, perfil software, perfil hardware.

Mathematics Subject Classification 2000: 94A60, 94A55, 11T71

¹Instituto de Física Aplicada
C.S.I.C.
Serrano 144, 28006 Madrid, España
amparo@iec.csic.es

²ITBA Instituto Tecnológico de Buenos Aires
Av. E. Madero 399, (C1106ACD)
Buenos Aires, Argentina
eugepazorobles@gmail.com

^{*}Trabajo realizado en el marco del proyecto HESPERIA: <http://www.proyecto-hesperia.org> financiado por el Centro para el Desarrollo Tecnológico Industrial (CDTI) a través del programa CENIT y por las empresas: INDRA, Unión Fenosa, TecnoBit, Visual-Tools, BrainStorm, SAC y TechnoSafe.

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Seguridad Matemática en Redes Ad-hoc Vehiculares

Pino Caballero Gil¹

El objetivo principal de este trabajo consiste en ofrecer un estado del arte de la comunicación cooperativa y segura en las conocidas como redes ad-hoc vehiculares o VANETs (Vehicular Ad-hoc NETworks), así como la descripción de algunos resultados preliminares obtenidos en este tema. En este trabajo se analizan diversos algoritmos criptográficos usados para afrontar dos de los problemas más importantes de la seguridad en redes inalámbricas en general y en VANETs en particular: la protección de la confidencialidad y el control de la autenticidad.

La mayoría de propuestas existentes para autenticación en VANETs implican el uso de firmas digitales adjuntando los certificados correspondientes emitidos por una Autoridad de Certificación. Sin embargo, esta solución sobrecarga en exceso el consumo de recursos [RAH06], dificulta el anonimato y conlleva la problemática asociada a la distribución de claves. Debido a lo extensas que son estas redes y a la necesidad de que las claves sean actualizadas con cierta frecuencia, para con ello proteger la privacidad, se hace impracticable que todos los vehiculos contengan las claves públicas del resto. En este trabajo proponemos un esquema de confianza basado en el modelo PGP que presta especial atención a la tarea de construcción de repositorios de certificados. Además la definición de la propuesta se apoya sobre un mecanismo de fomento de la cooperación entre nodos que tiene en cuenta especialmente la adaptación a la topología dinámica de la red.

En cuanto a la confidencialidad, dado que la criptografía asimétrica es en general muy costosa, y en las VANETs uno de los modos de operación se basa en el envío periódico de señales, la propuesta que se hace en este trabajo es la implementación de los cifrados más usados en redes inalámbricas, que son, por razones obvias de eficiencia, los cifrados en flujo. Se describe la fase de establecimiento de clave secreta compartida basado en el uso puntual de firma digital.

Keywords: Seguridad, VANETs, Criptografía

Mathematics Subject Classification 2000: 94A60, 94A6, 11T71

¹Dpto. Estadística, Investigación Operativa y Computación
Facultad de Matemáticas, Universidad de La Laguna
C/ Astrofísico Francisco Sánchez. 38271 La Laguna. Tenerife
pcaballe@ull.es

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Códigos de evaluación definidos por valoraciones

Carlos Galindo¹

En los 80 Goppa construyó códigos (lineales) correctores de errores usando herramientas de la Geometría Algebraica, lo que dió lugar a los llamados códigos algebro-geométricos que han adquirido gran notoriedad en los últimos años. Para tratar algunos de estos códigos de un modo más elemental, Hoholdt, van Lint y Pellikaan [3] introdujeron el concepto de función orden así como el de códigos de evaluación asociados a ellas. En la charla, revisaremos algunas contribuciones recientes a la teoría de códigos en esta línea, haciendo especial énfasis en trabajos conjuntos con M. Sanchis y F. Monserrat [2, 1] que permiten obtener buenos códigos utilizando en su construcción una superficie en lugar de una curva como lugar de elección de puntos a evaluar y una valoración asociada al anillo local de la superficie en un punto regular para construir la función orden que proporciona el código. Es especialmente interesante el caso en que se toman valoraciones en el infinito.

Keywords: Funciones orden, códigos de evaluación, valoraciones planas, valoraciones en el infinito

Mathematics Subject Classification 2000: 94B27, 14B05, 11T71

Referencias

- [1] C. GALINDO, F. MONSERRAT. δ -sequences and evaluation codes defined by plane valuations at infinity. *Proc. London Math. Soc.* doi:10.1112/plms/pdn042, 2008.
- [2] C. GALINDO, M. SANCHIS. Evaluation codes and plane valuations. *Des. Codes Crypt.* **41** 199–219, 2006.
- [3] T. HOHØLDT, J.H. VAN LINT, R. PELLIKAAN. *Algebraic geometry codes*. Handbook of coding theory, vol. 1, 871–961, 1998.

¹Departamento de Matemáticas
Universidad Jaume I
ESTCE. Campus Riu Sec. 12071 Castellón
galindo@mat.uji.es

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Códigos algebraico-geométricos sin geometría algebraica

Carlos Munuera López¹

Los códigos algebraico-geométricos fueron introducidos por Goppa en 1980. Su construcción se realiza a partir de una curva X definida sobre un cuerpo finito y dos divisores, y la geometría algebraica (Teoremas de Riemann-Roch, residuos, etc.) gobierna su comportamiento. A pesar de proporcionar códigos con excelentes parámetros, esta familia es escasamente utilizada en la práctica, en gran parte debido a la dificultad y el rechazo que provoca en los ingenieros. Por esa razón, a partir de los años 90 comenzaron a producirse intentos de describir estos códigos 'en términos elementales', es decir, utilizando únicamente funciones orden y semigrupos. Describimos algunos de los episodios relevantes en este proceso (aún inacabado) así como nuestra participación en ellos.

Keywords: Códigos correctores de errores, códigos algebraico-geométricos, semigrupos

Mathematics Subject Classification 2000: 94B27

¹Dpto. Matemática Aplicada. ETS Arquitectura
Avenida de Salamanca s/n
47014 Valladolid
cmunuera@arq.uva.es

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Criptografía con curvas elípticas

Anna Rio

Se trata de mostrar el uso criptográfico de las curvas elípticas, tanto en las aplicaciones ya plenamente comercializadas como en las propuestas que se hallan en proceso de investigación. Dicho uso criptográfico hace que las cuestiones deban abordarse siempre desde el punto de vista de la complejidad de los algoritmos de que disponemos para resolver determinados problemas matemáticos.

Keywords: Curva elíptica, complejidad, firma digital, algoritmo SEA.

Mathematics Subject Classification 2000: 11G20.

Referencias

- [1] N. KOBLITZ. *Elliptic curve cryptosystems. Mathematics of Computation*, **48**, 203–209, 1987.
- [2] V. MILLER. *Uses of Elliptic Curves in Cryptography. Advances in Cryptology-Crypto'85, Lecture Notes in Computer Science*, **218**, 417–426, 1986.
- [3] J. MIRET, R. MORENO, A. RIO AND M. VALLS. *Determining the 2-Sylow subgroup of an elliptic curve over a finite field. Mathematics of Computation*, **74**, 411–427, 2005.
- [4] J. MIRET, R. MORENO AND A. RIO. *Generalization of Vélu's formulae for isogenies. Publicacions Matemàtiques, Proceedings of the Primeras Jornadas de Teoría de Números*, 147–163, 2007.
- [5] J. MIRET, R. MORENO, A. RIO AND M. VALLS. *Computing the ℓ -power torsion of an elliptic curve over a finite field. Mathematics of Computation*, por aparecer. Article electronically published on October 29, 2008.
- [6] R. SCHOOF. *Elliptic curves over finite fields and the computation of square roots mod p . Mathematics of Computation*, **44**, 483–494, 1985.
- [7] J. VÉLU. *Isogénies entre courbes elliptiques. C. R. Acad. Sc. Paris*, **273**, 238–241, 1971.

Departamento de Matemática Aplicada II
Universidad Politécnica de Cataluña
Jordi Girona, 1-3. E-08034 Barcelona
ana.rio@upc.edu

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Criptografía con curvas hiperelípticas de género 2*

L. Hernández Encinas, J. Muñoz Masqué¹,

En el presente trabajo se presentan las clases de isomorfismo de las curvas hiperelípticas de género 2, que admiten un punto de Weierstrass (ver [6]). Dicha clasificación se ha llevado a cabo según que la característica del cuerpo sea 2 ([1, 2, 3]), 5 ([5]) o diferente de 2 y de 5 ([4]). Se ha determinado el número de curvas hiperelípticas que existen en cada uno de los casos mencionados. Este hecho tiene gran importancia desde el punto de vista de la criptografía, dado que para la implementación de posibles criptosistemas o protocolos de firma digital basados en tales curvas, esta clasificación permite conocer a priori el número de curvas diferentes, desde el punto de vista criptográfico, de que se dispone.

Keywords: Criptografía de clave pública, Cuerpos finitos, Curvas hiperelípticas, Clases de isomorfismo.

Mathematics Subject Classification 2000: 11G20, 94A60, 12E20.

Referencias

- [1] Y. CHOIE AND E. JEONG. Isomorphism classes of hyperelliptic curves of genus 2 over \mathbb{F}_{2^n} , *Cryptology ePrint Archive* 2003/213.
- [2] Y. CHOIE AND D. YUN. Isomorphism classes of hyperelliptic curves of genus 2 over \mathbb{F}_q , *Lect. Notes Comput. Sci.* **2384**, 190–202, 2002.
- [3] Y. DENG AND M. LIU. Isomorphism classes of hyperelliptic curves of genus 2 over finite fields with characteristic 2, *Science in China, Ser. A* **49**(2), 173–184, 2005.
- [4] L. HERNÁNDEZ ENCINAS, A.J. MENEZES, AND J. MUÑOZ MASQUÉ. Isomorphism classes of genus-2 hyperelliptic curves over finite fields, *Appl. Algebra Engrg. Comm. Comput.* **13**, 57–65, 2002.
- [5] L. HERNÁNDEZ ENCINAS AND J. MUÑOZ MASQUÉ. Isomorphism classes of genus-2 hyperelliptic curves over finite fields \mathbb{F}_{5^m} , *Information* **8**(6), 837–844, 2005
- [6] N. KOBLITZ. Hyperelliptic cryptosystems, *J. Cryptology* **1**, 139–150, 1989.

¹Departamento Tratamiento de la Información y Codificación
Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas
C/ Serrano 144, 28006-Madrid
{luis, jaime}@iec.csic.es

*Trabajo financiado por el CDTI, Ministerio de Industria, Turismo y Comercio, en colaboración con Telefónica I+D con el proyecto SEGUR@, de referencia CENIT-2007 2004.

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Configuraciones Combinatóricas y Recuperación Privada de Información por Pares

Maria Bras-Amorós, Josep Domingo-Ferrer, Klara Stokes

Los sistemas de recuperación privada de información (PIR) propuestos en la literatura requieren la cooperación de la base de datos. No obstante es el usuario quien está interesado en preservar su privacidad, mientras que el interés que pueda tener la base de datos en el PIR es muy dudoso. La recuperación privada de información por pares (P2P PIR) constituye un enfoque más práctico: un grupo de usuarios se ayudan unos a otros a someter sus consultas, con lo cual consiguen privacidad sin cooperación de la base de datos. Una forma de implementar el P2P PIR se basa en el uso de configuraciones combinatorias para la gestión de las claves necesarias para la comunicación privada entre los pares[1, 2]. Este artículo explora dicho enfoque y se ocupa de la construcción de configuraciones óptimas, las cuales resultan ser grafos de Ramanujan.

Keywords: Configuración combinatoria, recuperación privada de información, grafos de Ramanujan

Mathematics Subject Classification 2000: 94A60, 05B30, 05Cxx

Referencias

- [1] J. DOMINGO-FERRER AND M. BRAS-AMORÓS. Peer-to-peer private information retrieval. In *Privacy in Statistical Databases-PSD 2008*, J. Domingo-Ferrer and Y. Saygin (eds.), pp. 315–323. *Lecture Notes in Computer Science*, vol. 5262, Springer-Verlag, Berlin, 2008.
- [2] J. DOMINGO-FERRER, MARIA BRAS-AMORÓS, QIANHONG WU AND JESÚS MANJÓN. Private information retrieval based on a peer-to-peer community. *Data and Knowledge Engineering* (to appear).

¹Càtedra UNESCO de Privadesa de Dades
Departament d'Enginyeria Informàtica i Matemàtiques
Universitat Rovira i Virgili
Av. Països Catalans 26, 43007 Tarragona
{maria.bras,josep.domingo,klara.stokes}@urv.cat

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Aspectos criptográficos de algunas secuencias pseudoaleatorias

Domingo Gómez¹

Las secuencias que son generados por algoritmos deterministas para simular secuencias verdaderamente aleatorias se las denomina pseudoaleatorias. Las secuencias pseudoaleatorias son utilizadas en diferentes campos, desde la simulación hasta el análisis numérico, nuestra motivación es la criptología. Hay muchas situaciones en criptografía donde es importante ser capaz de generar números aleatorios, cadenas de bits, etc. La generación de números aleatorios lanzando monedas u otros procesos físicos es muy costosa, por lo que en la práctica es común utilizar generadores de números pseudoaleatorios. Un generador de números pseudoaleatorios (PRNG) es un algoritmo para generar una secuencia de números que se aproxima a las propiedades de los números aleatorios. La secuencia no es verdaderamente aleatoria en el sentido de que está totalmente determinado por un relativamente conjunto pequeño de valores iniciales, llamado el estado del PRNG.

Existen varias medidas de calidad de la aleatoriedad de las secuencias de acuerdo con el tipo de problema donde las secuencias pseudoaleatorias se utilicen. Debido a la amplia gama de este campo, sólo trataremos PRNG con aplicaciones a la criptografía. En esta charla presentaremos resultados recientes acerca de la discrepancia y el perfil de la complejidad lineal de algunas secuencias pseudoaleatorias.

Keywords: secuencias pseudoaleatorias, perfil de la complejidad lineal, discrepancia, criptografía.

Mathematics Subject Classification 2000: 11T71, 11T6, 11T23

¹Departamento de Matemáticas, Estadística y Computación
Universidad de Cantabria
Avenida de Los Castros s/n, Santander
domingo.gomez@unican.es

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Verificabilidad en Criptografía

Jorge L. Villar¹

En esta charla se analiza las diferentes manifestaciones de la verificabilidad en criptografía, tanto como parte integrante de las especificaciones del protocolo (como en el caso de la firma digital), como por las diferentes técnicas para conseguirla (por ejemplo, pruebas de conocimiento cero y uso de emparejamientos) y su aplicación a la mejora de las demostraciones de seguridad por reducción.

La charla se divide básicamente en tres secciones, correspondientes a las diferentes facetas de la criptografía en las que la verificabilidad ocupa un papel importante. En la primera sección se estudia la verificabilidad de los textos cifrados en un criptosistema de clave pública como herramienta para alcanzar la seguridad IND-CCA, y la manera en que la verificabilidad puede afectar a las demostraciones de seguridad por reducción.

La segunda sección se ocupa de los esquemas de firma digital, en los que la verificabilidad aparece como parte esencial de su definición. Es por ello que en los esquemas de firma digital es donde se puede ver el abanico de técnicas usadas en criptografía para garantizar la verificabilidad.

La tercera sección está dedicada a los protocolos distribuidos y al papel de la verificabilidad en los esquemas para compartir secretos.

Keywords: Verificabilidad, Seguridad CCA, Firma de Contratos, Emparejamientos, Compartición de Secretos

Mathematics Subject Classification 2000: 94A60

¹Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Jorge Girona 1-3, 08034 BARCELONA
jvillar@ma4.upc.edu

Congreso de la Real Sociedad Matemática Española
Oviedo, 4 a 7 de febrero de 2009

Sobre algunas construcciones de funciones bent

Joan-Josep Climent¹, Francisco J. García², Verónica Requena¹

La implementación de una caja de sustitución o S-box necesita funciones booleanas no lineales para resistir ataques tales como el criptoanálisis diferencial. Para un número par de variables, las funciones booleanas de máxima no linealidad son las llamadas funciones *bent*.

Recordemos que una **función booleana** de n variables es una aplicación $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$. Un **minterm** en las variables x_1, x_2, \dots, x_n es la función booleana dada por

$$m_{(u_1, u_2, \dots, u_n)}(x_1, x_2, \dots, x_n) = (1 \oplus u_1 \oplus x_1)(1 \oplus u_2 \oplus x_2) \cdots (1 \oplus u_n \oplus x_n)$$

donde $(u_1, u_2, \dots, u_n) \in \mathbb{Z}_2^n$. Para $i = 0, 1, 2, \dots, 2^n - 1$, es evidente que $m_{\mathbf{e}_i}(\mathbf{x}) = 1$ si y sólo si $\mathbf{x} = \mathbf{e}_i$, donde \mathbf{e}_i es la expansión binaria de i . Cuando no haya lugar a confusión, escribiremos $m_i(\mathbf{x})$ en lugar de $m_{\mathbf{e}_i}(\mathbf{x})$.

En este trabajo se revisan las construcciones de funciones bent de Rothaus y de Maiorana-McFarland y se introducen dos construcciones nuevas basadas en los resultados siguientes. Aquí $\mathbf{y} = (y_1, y_2)$ es un vector de dos variables.

Teorema 1 *Supongamos que $f_0(\mathbf{x})$ y $f_1(\mathbf{x})$ son funciones bent de n variables y que (i_0, i_1, i_2, i_3) es una permutación cualquiera de $(0, 1, 2, 3)$. Entonces*

$$F(\mathbf{y}, \mathbf{x}) = (m_{i_0}(\mathbf{y}) \oplus m_{i_1}(\mathbf{y})) f_0(\mathbf{x}) \oplus m_{i_2}(\mathbf{y}) f_1(\mathbf{x}) \oplus m_{i_3}(\mathbf{y}) (1 \oplus f_1(\mathbf{x}))$$

es una función bent de $n + 2$ variables.

Teorema 2 *Sea $f(\mathbf{x})$ una función bent de n variables y consideremos $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$. Si (i_0, i_1, i_2, i_3) es una permutación cualquiera de $(0, 1, 2, 3)$, entonces*

$$G(\mathbf{y}, \mathbf{x}) = m_{i_0}(\mathbf{y}) f(\mathbf{x}) \oplus m_{i_1}(\mathbf{y}) f(\mathbf{x} \oplus \mathbf{u}) \oplus m_{i_2}(\mathbf{y}) f(\mathbf{x} \oplus \mathbf{v}) \oplus m_{i_3}(\mathbf{y}) (1 \oplus f(\mathbf{x} \oplus \mathbf{u} \oplus \mathbf{v}))$$

es una función bent de $n + 2$ variables.

Keywords: Función booleana, minterm, no linealidad, función bent

Mathematics Subject Classification 2000: 06E30, 94A60

¹Departament de Ciència de la Computació i Intel·ligència Artificial
Universitat d'Alacant
Campus de Sant Vicent del Raspeig, Ap. correus 99, 03080 Alacant
{jcliment, vrequena}@ua.es

²Departament de Fonaments de l'Anàlisi Econòmica
Universitat d'Alacant
Campus de Sant Vicent del Raspeig, Ap. correus 99, 03080 Alacant
francisco.garcia@ua.es

Índice alfabético

Borges, J., 4
Borges-Quintana, M., 3
Borges-Trenard, M.A., 3
Bras-Amorós, Maria, 11

Caballero Gil, Pino, 6
Climent, Joan-Josep, 14

Domingo-Ferrer, Josep, 11

Fúster Sabater, A., 5

Gómez, Domingo, 12
Galindo, Carlos, 7
García, Francisco J., 14

Hernández Encinas, L., 10

Martínez-Moro, E., 3
Muñoz Masqué, J., 10
Munuera López, Carlos, 8

Pazo Robles, M.E., 5

Requena, Verónica, 14
Rifà, J., 4
Rio, Anna, 9

Stokes, Klara, 11

Villanueva, M., 4
Villar, Jorge L., 13