SESIONES ESPECIALES

Congreso RSME 2013

S16
Matemáticas de la Teoría de la Información

Mar 22, 17:00 - 17:35, Aula 9 – Carlos Munuera:
Ocultando la información: la Esteganografía

Mar 22, 17:40 - 18:15, Aula 9 – Marta Pujol:
Fountain Codes

Mar 22, 18:20 - 18:55, Aula 9 – Joan Josep Climent:
Construcción de funciones bent de $2k$ variables a partir de una base de F_2^{2k}

Mar 22, 19:00 - 19:35, Aula 9 – José María Muñoz Porras:
Sobre una familia de Códigos Convolucionales 1-dimensionales que son Códigos de Goppa

Mie 23, 11:00 - 11:35, Aula 9 – Diego Ruano:
Feng-Rao decoding of primary codes

Mie 23, 11:40 - 12:15, Aula 9 – Magdalena Payeras Capellà:
Criptografía y medios de pago electrónicos

Mie 23, 12:20 - 12:55, Aula 9 – Andreu Pere Isern:
Implementación de las firmas de grupo basadas en las "pairing functions"

Mie 23, 17:00 - 17:35, Aula 9 – Llorenç Huguet:
Secreto y Autenticación perfectos

Mie 23, 17:40 - 18:15, Aula 9 – Anna Río:
Identidad digital

Mie 23, 18:20 - 18:55, Aula 9 – Josep Domingo Ferrer:
Coutilidad: teoría y aplicaciones

Mie 23, 19:00 - 19:35, Aula 9 – Josep María Miret:
Códigos secretos: de Turing a la criptografía de clave pública

Jue 24, 11:00 - 11:35, Aula 6 – Simeon Ball:
Results on error-correcting codes obtained using linear algebra

Jue 24, 11:40 - 12:15, Aula 6 – Irene Márquez Corbella:
Enfoque algebraico a la descodificación de códigos lineales

Jue 24, 12:20 - 12:55, Aula 6 – Oriol Farrás Ventura:
Esquemas de compartición de secretos para grafos

Jue 24, 13:00 - 13:35, Aula 6 – Josep Rifá:
Hadamard quaternionic codes

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Ocultando la información: la Esteganografía

Carlos Munuera[1]

En los últimos años ha ido cobrando importancia, como alternativa y como complemento de la criptografía, una antigua técnica de protección de la información: la esteganografía. Su propósito es esconder la información (en lugar de hacerla ilegible). En esta comunicación expondremos los principios generales en los que se basa, haciendo especial hincapié en su relación con la teoría de códigos correctores de errores.

[1]Universidad de Valladolid
cmunuera@arq.uva.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Fountain Codes

Marta Pujol[1]

Fountain codes are a class of sparse-graph erasure codes. They produce a potentially limitless stream of output symbols (generated randomly) with the property that the original source symbols can be recovered from any subset of the output symbols of size slightly larger than the number of source symbols. The main codes Tornado, LT and Raptor and their properties are introduced. New lines of research based on these codes are presented.

[1]Universitat Rovira i Virgili

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Construcción de funciones bent de $2k$ variables a partir de una base de $\mathbb{F}_2^{2k}$

Joan Josep Climent[1]

Sea k un entero positivo y $\mathbb{F}_2$ el cuerpo de dos elementos 0 y 1. A partir de una base del espacio vectorial $\mathbb{F}_2^{2k}$ construimos subconjuntos de $\mathbb{F}_2^{2k}$ que resultan ser los soportes de funciones bent de $2k$ variables.

[1]Universitat d'Alacant.
jcliment@ua.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Sobre una familia de Códigos Convolucionales 1-dimensionales que son Códigos de Goppa

José María Muñoz Porras[1]

Se propone un método general para construir códigos convolucionales MDS de dimensión 1. Este método generaliza construcciones previas realizadas por Gluesing-Luerssen y Langfeld. Estas construcciones permiten clasificar los códigos convolucionales de Goppa de dimensión 1.

[1]Universidad de Salamanca.
jmp@usal.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Feng-Rao decoding of primary codes

Diego Ruano[1]

We show that the Feng-Rao bound for dual codes and a similar bound by Andersen and Geil [H.E. Andersen and O. Geil, Evaluation codes from order domain theory, Finite Fields Appl., 14 (2008), pp. 92-123] for primary codes are consequences of each other. This implies that the Feng-Rao decoding algorithm can be applied to decode primary codes up to half their designed minimum distance. The technique applies to any linear code for which information on well-behaving pairs is available.

Among those are important families of multivariate polynomial codes. Matsumoto and Miura in [R. Matsumoto and S. Miura, On the Feng-Rao bound for the L-construction of algebraic geometry codes, IEICE Trans. Fundamentals, E83-A (2000), pp. 926-930] (See also [P. Beelen and T. Høholdt, The decoding of algebraic geometry codes, in Advances in algebraic geometry codes, pp. 49-98]) derived from the Feng-Rao bound a bound for primary one-point algebraic geometric codes and showed how to decode up to what is guaranteed by their bound. The exposition by Matsumoto and Miura requires the use of differentials which was not needed in [Andersen and Geil 2008]. Nevertheless we demonstrate a very strong connection between Matsumoto and Miura's bound and Andersen and Geil's bound when applied to primary one-point algebraic geometric codes.

(Joint work with Olav Geil (Aalborg University) and Ryutaroh Matsumoto (Tokyo Institute of Technology)

[1]Aalborg Universitet.
diego@math.aau.dk

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Criptografía y medios de pago electrónicos

Magdalena Payeras Capellà[1]

La seguridad en los sistemas de pago tradicionales se basa en mecanismos físicos que impiden su falsificación y uso fraudulento. En los sistemas de pago electrónicos la seguridad se consigue mediante el uso de criptografía. En concreto, las firmas digitales en todas sus variantes permiten obtener características deseables en los sistemas de pago electrónicos para las nuevas aplicaciones y servicios que van desarrollándose en el entorno del comercio electrónico. Entre estas aplicaciones se encuentran la compra de información o de bienes digitales de bajo coste o el acceso a servicios tarificables en función de su uso. Tanto en un servicio como en el otro la privacidad del usuario es una propiedad deseable.

En el primer caso, la compra de bienes de bajo precio requiere un sistema de pago adaptado al pago de pequeñas cantidades, llamado micropago, con requerimientos de seguridad, de eficiencia y funcionales únicos dentro del abanico de sistemas de pago existentes. En el segundo caso, la tarificación en función del uso se realizará de forma automática, dando lugar a sistemas de tarificación automática.

Las firmas ciegas permiten crear monedas electrónicas anónimas. Sin embargo en determinados casos se requerirán firmas con propiedades adicionales, como firmas parcialmente ciegas o firmas de grupo. Las firmas parcialmente ciegas permiten al firmante introducir información común, previamente acordada entre solicitante y firmante, en la firma ciega. Las firmas de grupo pueden ser útiles para verificar que el usuario firmante es miembro de un determinado grupo de usuarios. Los tiques electrónicos (de tarificación preestablecida o automática) pueden ser emitidos de forma anónima incorporando firmas de grupo en su etapa de generación. Los esquemas de firma de grupo permiten la revocación de la identidad de los usuarios in caso de comportamiento incorrecto.

La incorporación de medidas de seguridad y privacidad a los sistemas de pago electrónico requiere gran volumen de computación. Por tanto su aplicabilidad a determinados dispositivos, como dispositivos móviles, debe ser comprobada.

[1]Universitat Illes Balears.
mpayeras@uib.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Implementación de las firmas de grupo basadas en las "pairing functions"

Andreu Pere Isern (Con Llorenç Huguet, Magdalena Payeras, Macià Mut)[1]

En esta presentación, vamos a mostrar una aplicación de las "pairing functions" a la firma de grupo, según el esquema propuesto por Boneh, Boyen y Shacham (BBS) [1], válida tanto para portátiles convencionales como para teléfonos inteligentes que disponen del sistema operativo Android.

Los esquemas de firma de grupo fueron introducidas por D. Chaum y E.V.Van Heyst (1991) [2] para proporcionar, al mismo tiempo, la autenticidad y el anonimato de los usuarios. Así, con un par clave de grupo, cada usuario perteneciente al grupo puede firmar mensajes que son públicamente verificables, al mismo tiempo que oculta la identidad del firmante real dentro del grupo. De esta forma, la firma resultante mantiene en secreto la identidad del firmante, debido a que el procedimiento de verificación sólo emplea la clave pública del grupo. Sólo el administrador del grupo, en el caso de cualquier conflicto o abuso, puede rastrear la firma, deshaciendo su anonimato.

En este trabajo, presentaremos la implementación del esquema de firma de grupo BBS, basado en "pairing functions", cuyo análisis de rendimiento permite visualizar la importancia de estas firmas para las aplicaciones criptográficas en general, como para las que requieran dispositivos móviles.

Referencias

[1] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In Advances in Cryptology – CRYPTO 2004, volume 3152 of Lecture Notes in Computer Science, page 227–242. 2004.

[2] D. Chaum and E.V. Van Heyst. Group signatures. In Proceedings of the 10th annual International Conference on Theory and Application of Crypto- graphic Techniques, EUROCRYPT'91, page 257–265, 1991.

[1]Universitat d'Illes Balears.

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Secreto y Autenticación perfectos

Llorenç Huguet[1]

El concepto de secreto perfecto fue estudiado por C.E. Shannon (1949) [2], quien lo caracterizó como el máximo de incertidumbre para un criptoanalista sobre el texto original, una vez interceptado el texto cifrado. En términos de teoría de la información equivale a conseguir un sistema donde la información mutua entre emisor y criptoanalista sea nula. Es decir, si para un sistema criptográfico determinado, M es el conjunto de mensajes originales y C el conjunto de los mensajes cifrados entonces habrá secreto perfecto cuando $I(M, C) = H(M|C) = H(M) = 0$. Operando sobre las propiedades de las funciones de entropía, se deduce que el secreto perfecto de Shannon se consigue cuando la clave requiere al menos, el mismo número de bits que el mensaje a cifrar. El único criptosistema conocido que cumple esta condición es el de Vernam.

El criptosistema coset-coding para wire-Tap channels, que presentaremos, visando el secreto perfecto da un esquema de cifrado que al mismo tiempo maximiza la información mutua entre el emisor y el receptor legal.

Puesto que la criptografía además de asegurar el secreto de las transmisiones y/o almacenamiento de datos, pretende asegurar la autenticación de los usuarios, G.S. Simmons (1984) [3], presenta una teoría de la autenticación perfecta, siguiendo la teoría de la información. Su resultado es que existe la autenticación perfecta cuando el ataque de personalización verifica que la probabilidad de engaño por parte de un criptoanalista $P_e = 2^{-I(C,K)}$, donde $I(C, K)$ es la información mutua entre el conjunto de criptogramas y el conjunto de claves posibles para el criptosistema.

El secreto y la autenticación son conceptos independientes entre si; pueden existir criptosistemas con secreto perfecto y sin autenticación y otros con autenticación perfecta y sin secreto.

Referencias

[1] Comunicación digital: teoría matemática de la información, codificación algebraica y criptología Ed. Masson, 1991.

[2] C.E. Shannon. Communication theory of secrecy systems. Bell Syst. Tech., 28:656–715, 1949.

[3] G.S. Simmons. Authentication theory/ coding theory. In Crypto'84, Lecture Notes in Computer Science. volume 196 pages 411–431.

[1]Universitat d'Illes Balears.
l.huguet@uib.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Identidad digital

Anna Río[1]

Los números nos identifican. Estamos acostumbrados a ello: número de teléfono, número de identificación fiscal, número de la tarjeta de crédito, etc. Pero, sin presencia física ¿cómo podemos estar seguros de que un número corresponde realmente a una identidad?

Los negocios o acuerdos buenos y perdurables han incluido siempre el reconocimiento físico, el contacto visual, el establecimiento de vínculos personales. Por lo tanto, el reconocimiento y la subsiguiente autenticación de la persona o entidad con la que realizar negocios o cualquier tipo de transacción o interacción importante se convierte en la piedra angular de la relación.

Se establece así confianza entre los participantes, y la confianza es la base de las relaciones. Cuando la tecnología pretende convertirse en un substituto viable para la interacción física humana adquieren gran relevancia los conceptos de identidad digital y autenticación digital. Con el fin de estandarizar estas formas de identificación, gobiernos, organizaciones y empresas han emitido, o lo harían en un futuro inmediato, sus propias tarjetas de identidad digital. Estas tarjetas de identidad electrónicas tienen un microchip cuya memoria y potencia de cálculo se utilizan para incorporar algoritmos criptográficos, lo que permite la autenticación y la firma digital.

Revisaremos algunas de las matemáticas que intervienen en estas infraestructuras, considerando diferentes elecciones posibles. Entendiendo sus características y su funcionamiento, podremos convencernos y convencer de que las tecnologías de la información y las comunicaciones son capaces de hacer identificaciones fiables entre empresas, entre empresas y clientes, entre gobiernos y ciudadanos, etc. garantizando que la información crítica y sensible se mantiene siempre bajo control de su propietario.

[1]Universitat Politècnica de Catalunya.
ana.rio@upc.edu

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Coutilidad: teoría y aplicaciones

Josep Domingo Ferrer[1]

Un problema existente en la sociedad de la información global es la falta de un marco legal aceptado por todos los países. Ello conlleva el problema de proteger los intereses legítimos de los participantes en transacciones de información. Los protocolos usados en la sociedad de la información deberían diseñarse para que el interés egoísta de cualquier participante le lleve a actuar de tal modo que sirva al interés de los otros participantes. De esta forma, la sociedad de la información podrá funcionar como resultado de una cooperación autointeresada en lugar de basarse en preceptos legales difíciles de desplegar.

La coutilidad es un nuevo concepto que puede definirse en términos de teoría de juegos: un protocolo es coútil si la mejor opción que tiene un participante para maximizar su utilidad es cooperar con uno o más de los otros participantes para maximizar la utilidad de estos. Es cuestión de ayudarse a uno mismo a base ayudar a otros. La privacidad, la seguridad y la funcionalidad pueden verse como componentes básicos de la utilidad de un participante.

Definimos formalmente la coutilidad en términos de equilibrio de juegos. Pueden considerarse varios tipos de equilibrio: i) si los jugadores/participantes juegan de forma independiente, la coutilidad se define como un equilibrio de Nash de un subjuego, también conocido como equilibrio de Stackelberg; ii) si se permite que los jugadores correlacionen sus estrategias para mejorar el resultado final, obtenemos coutilidad correlacionada definida como un equilibrio correlacionado.

En esta charla presentaremos varios aspectos teóricos de la coutilidad y esbozaremos algunas de sus aplicaciones: distribución controlada de contenidos, olvido digital, búsqueda anónima de información, comunicaciones en redes vehiculares y redes sociales.

[1]Universitat Rovira i Virgili
josep.domingo@urv.cat

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Códigos secretos: de Turing a la criptografía de clave pública

Josep María Miret[1]

Desde que Alan M. Turing (1912-1954), con su colaboración con el servicio secreto británico durante la segunda guerra mundial, condujo a descifrar los códigos producidos por la máquina criptográfica del ejército alemán denominada Enigma, hasta la era actual de los ordenadores, la criptografía ha experimentado un espectacular avance y un fascinante desarrollo. En esta charla mostraremos las características de algunos criptosistemas, tanto de clave compartida como de clave pública, aparecidos después del célebre artículo de 1949 de C. Shannon donde se establecen los pilares de la criptografía moderna. Comentaremos también, algunos de los posibles ataques criptoanalíticos que intentan cuestionar y romper su seguridad. Finalmente, veremos que la criptografía con emparejamientos ofrece buenas propiedades para evitar el uso de certificados de claves públicas.

[1]Universitat de Lleida.
miret@matematica.udl.cat

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Results on error-correcting codes obtained using linear algebra

Simeon Ball[1]

A linear code C is a k-dimensional subspace of $\mathbb{F}_q^n$, with respect to a fixed basis. Let $d \in \mathbb{N}$ be minimal sich that every non-zero vector of C has at least d non-zero coordinates. With such a code, up to $\lfloor (d-1)/2 \rfloor$ errors in any codeword can be corrected when sending codewords down a noisy channel.

There are many results on error-correcting codes obtained by combinatorial arguments (and these generally apply to non-linear codes as well) such as the sphere packing bound, the Gilbert-Varshamov bound, the Plotkin bound, etc. In this talk I will concentrate on results obtained using linear algebra, for example the MacWilliam's identities, the MDS conjecture, the maximum weight of a codeword. It is also possible to obtain results for non-linear codes using linear algebra and I will also mention one of these, the Alderson-Gács extension theorem.

[1]Universitat Politècnica de Catalunya.
simeon@ma4.upc.edu

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Enfoque algebraico a la descodificación de códigos lineales

Irene Márquez Corbella[1]

En esta charla introducimos el ideal binomial asociado a un código lineal arbitrario. Los binomios de la base de Gröbner de dicho ideal respecto de un orden graduado inducen un conjunto de prueba o "test-set" que nos permite resolver el problema de descodificación completa de códigos lineales. Por otra parte la base de Graver de este ideal nos aporta un test-set universal que resulta contener el conjunto de palabras de mínimo soporte de nuestro código.

En el caso binario algunos de estos resultados ya se conocían. Presentamos aquí extensiones de los algoritmos conocidos que nos permiten calcular, sin aumento del coste computacional, algunos parámetros del código como el conjunto de palabras líderes, su distribución de pesos o el radio de recubrimiento y de Newton del código. Podemos incluso hacer uso de la teoría de descomposición de matroides representables para reducir la complejidad de los algoritmos propuestos en ciertos casos.

[1]Universidad de Valladolid
imarquez@agt.uva.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Esquemas de compartición de secretos para grafos

Oriol Farrás Ventura[1]

Un esquema de compartición de secretos es un método criptográfico para dividir un secreto en fragmentos. Esta división se realiza de manera que a partir de ciertos conjuntos de fragmentos, los conjuntos "autorizados", es posible recuperar el secreto, mientras que los otros conjuntos de fragmentos no contienen ninguna información del secreto. La familia de conjuntos autorizados se llama estructura de acceso del esquema. Los esquemas de compartición de secretos son incondicionalmente seguros, su seguridad se basa en la teoría de la información, y son una primitiva fundamental en la construcción de aplicaciones criptográficas.

Existen procedimientos para construir esquemas de compartición de secretos para cualquier estructura de acceso monótona creciente. Pero en la mayoría de los casos el esquema resultante es ineficiente, la longitud de los fragmentos es exponencial en el número de participantes. Se conocen algunas familias de estructuras de acceso que admiten esquemas eficientes, pero en general no se sabe cual es la longitud mínima de los fragmentos para una estructura de acceso cualquiera.

Este problema ha sido abordado en un trabajo conjunto con Amos Beimel y Yuval Mintz, presentado en CRYPTO 2012. El estudio se ha restringido a las estructuras de acceso determinadas por grafos, y se han obtenido construcciones más eficientes y cotas inferiores en la longitud mínima de los fragmentos.

[1]Universitat Rovira i Virgili
oriol.fv@gmail.com

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Hadamard quaternionic codes

Josep Rifá (Con Ángel del Río, Murcia) [1]

A quaternionic code is a non-empty subgroup of Q^n, where Q is the quaternion group on eight elements. Such codes are translation invariant propelinear codes as the well known $Z4$-linear or $Z2Z4$-linear codes.

We will show that there exist "pure"' quaternionic codes, that is, codes that do not admit any abelian translation invariant propelinear structure. We study the dimension of the kernel and rank of the quaternionic codes, and we give upper and lower bounds for these parameters. We give tools to construct a new class of Hadamard codes formed by several families of quaternionic codes; we study and show the different shapes of such a codes and we improve the upper and lower bounds for the rank and the dimension of the kernel when the codes are Hadamard.

[1]Universitat Autonoma de Barcelona.
josef.rifa@uab.cat