CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

On asymptotically good ramp secret sharing schemes

Umberto Martínez-Peñas[1], **Olav Geil**[1], **Stefano Martin**[1], **Ryutaroh Matsumoto**[2], **Diego Ruano**[1]

Asymptotically good sequences of ramp secret sharing schemes have been intensively studied by Cramer et al. [2, 1]. In those works the focus is on full privacy and full reconstruction. We propose an alternative definition of asymptotically good sequences of ramp secret sharing schemes where a small amount of information leakage is allowed (and possibly also non-full recovery). By a non-constructive proof we demonstrate the existence of sequences that – following our definition of goodness – have parameters arbitrary close to the optimal ones. Moreover – still using our definition – we demonstrate how to concretely construct asymptotically good sequences of schemes from sequences of algebraic geometric codes related to a tower of function fields. Our study involves a detailed treatment of the relative generalized Hamming weights of the involved codes.

Referencias

[1] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan: Secure computation from random error correcting codes, *Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci.* **4515** (2007), 291–310.

[2] H. Chen and R. Cramer: Algebraic geometric secret sharing schemes and secure multi-party computations over small fields, *Advances in cryptology—CRYPTO 2006, Lecture Notes in Comput. Sci.* **4117** (2006), 291–310.

[1]Department of Mathematical Sciences
Aalborg University, Denmark
umberto@math.aau.dk

[2]Department of Communications and Computer Engineering
Tokyo Institute of Technology, Japan

La lucha antiterrorista a través de algoritmos algebraicos y estocásticos aplicados a los Servicios de Información

M. Pilar Velasco[1], **Álvaro Barreras**[1], **Simona Bernardi**[1], **Lacramioara Dranca**[1], **Pedro A. López**[2], **Antonio M. Oller**[1], **Francisco J. Umpiérrez**[2], **Rubén Vigara**[1]

Las bases de datos utilizadas por los Servicios de Información de la Guardia Civil manejan un volumen muy grande de información relativa a personas que directa o indirectamente se encuentran vinculadas a grupos terroristas, sin embargo dicha información presenta importantes dificultades de gestión y manejo debido precisamente al amplio contenido y a la difícil clasificación de los datos de entrada que es necesario almacenar y estudiar.

Por este motivo, es de gran importancia mejorar el tratamiento de la información a través de un estudio científico-tecnológico basado en algoritmos algebraicos y estocásticos. En dicho estudio analizamos diferentes técnicas con el objetivo final de desarrollar una herramienta software de apoyo a la toma de decisiones para los servicios de información de la lucha contra el terrorismo de forma que, ocurrido un atentado terrorista en un lugar determinado, permita obtener una lista con un reducido número de personas con alta probabilidad de implicación en dicho atentado.

CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

[1]Área de Matmáticas, Estadística e Investigación Operativa
Centro Universitario de la Defensa
Academia General Militar, Ctra. de Huesca s/n, 50090 Zaragoza
velascom@unizar.es

[2]Grupo de Reserva y Seguridad de Valencia (P. A. López)
Comandancia de Lugo (F. J. Umpiérrez)
Guardia Civil