I+D 2008
CSIC
Resumen de Proyecto

DATOS DEL PROYECTO
A) Análisis de Funciones Booleanas y sus Aplicaciones a la Criptografía.
B) Responsable: Alfredo Viola
C) Área: Básica Disciplina: Informática
D) Grado y Horas del responsable: Grado 5, 40 hs. DT
E) Facultad o Servicio: Ingeniería
F) Departamento o Instituto: Computación

Las funciones booleanas cumplen un papel estratégico en criptografía y códigos correctores de errores. Muchas aplicaciones criptográficas (generadores pseudoaleatorios en cifrados de flujo, "S-boxes" en cifrado en bloques) son designados usando composiciones apropiada de funciones booleanas no lineales.

La funciones booleanas deben cumplir varias propiedades criptográficas tales como resiliencia, grado algebraico o no-linealidad que permiten al diseñador de un sistema criptográfico cuantificar el nivel de resistencia frente a los ataques. Sin embargo, muchas de estas restricciones son muy difíciles (o en algunos casos hasta se puede demostrar la imposibilidad!) de cumplir simultáneamente. Por tal motivo, hay que encontrar soluciones de compromiso que permitan balancear propiedades que deben ser cuantificadas apropiadamente.

En este proyecto nos concentramos en una novedosa metodología combinatoria presentada por J.M Lebars (U. De Caen, Francia) y Alfredo Viola orientada a trabajar con funciones 1-resilientes. Como continuación, estamos trabajando en el uso de esta metodología para estudiar otro tipo de propiedades. Participaron también un estudiante de grado y un estudiante de Maestría. Los resultados alcanzados se pueden resumir en:

- Presentación de la novedosa metodología combinatoria.
- Conteo de funciones Booleanas 1-resiliente hasta 8 variables.
- Propuesta de un algoritmo de codificación enumerativa de funciones Booleanas 1-resilientes. Es la primera vez en la literatura científica que una biyección de estas características se presenta en un problema de funciones Booleanas con aplicaciones criptográficas.
- Como consecuencia, hemos presentado algoritmos eficientes de generación aleatoria de funciones Booleanas 1-resilientes de "n" variables.
- Implementación eficiente de estos algoritmos, que permiten en menos de 30 segundos generar una función 1-resiliente aleatoria de hasta 8 variables.