Demostrando Conocimiento de un Conjunto Independiente

Pino Caballero Gil

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

La noción de Demostración de Conocimiento Nulo (Zero Knowledge Proof, ZKP) ha sido hasta hoy una de las más estudiadas por la comunidad criptográfica. Tras su introducción en 1985, ha resultado ser muy útil tanto en Teoría de la Complejidad como en Criptografía, jugando en este último campo un papel fundamental para la construcción de protocolos criptográficos. Resulta llamativo que la mayoría de las ZKP que se han publicado hasta ahora están relacionadas con los mismos problemas, supuestamente difíciles, en los que la Criptografía de Clave Pública está basada.

El presente trabajo trata concretamente sobre las ZKP computacionales, cuya existencia fue demostrada en 1986 para cualquier problema NP, suponiendo la hipótesis de que existen funciones unidireccionales. En el mismo trabajo, los autores describieron una ZKP basada en el problema de la 3-coloración, y propusieron el uso de las reducciones para lograr una ZKP para cualquier otro problema NP. La eficiencia del algoritmo aquí propuesto proviene de un acercamiento diferente basado en un esquema específico diseñado para un problema concreto de forma que se evita el uso de reducciones generales mediante la combinación de la Teoría de Números y la Teoría de Grafos.

Uno de los resultados más relevantes con respecto a las ZKP fue la demostración de que la existencia de conocimiento nulo perfecto para algún problema NP-completo causaría el colapso de la Jerarquía de Tiempo Polinomial. Ya que la Teoría de Grafos es una fuente densa de problemas NP, varias ZKP para diferentes problemas de grafos tales como el isomorfismo, el no-isomorfismo, los circuitos hamiltonianos, y el conjunto independiente han sido propuestas en la literatura.

Sin embargo todas esas propuestas están relacionadas de alguna manera con el mismo problema básico, el Isomorfismo de Grafos. El inconveniente mayor de este hecho se debe a que la complejidad computacional concreta de dicho problema no se conoce todavía, e incluso el problema parece fácil para la mayoría de grafos

generados del azar. Por el contrario, el presente trabajo propone una nueva ZKP Computacional para el problema del Conjunto Independiente, cuya seguridad se basa en la dificultad del Problema del Logaritmo Discreto.