Criptografía basada en retículos

La Criptografía basada en retículos (del inglés Lattice-based cryptography) es un término genérico para la construcción de primitivas criptográficas que utilizan retículos, bien en la propia construcción, bien en la prueba de seguridad.

Las construcciones basadas en retículos son, en la actualidad, candidatos importantes para la denominada criptografía postcuántica, ya que, a diferencia de los esquemas de clave pública más utilizados, como son los RSA, Diffie-Hellman o la criptografía de curva elíptica, que pueden ser fácilmente atacables usando un computador cuántico, varias construcciones basadas en retículos parecen ser resistentes a los ataques basados tanto en computación cuántica como clásica.

Además, se ha demostrado que muchas construcciones basadas en retículos son seguras asumiendo que no es posible resolver de forma eficiente ciertos problemas bien conocidos de retículos.