# Esquemas de cifrado basados en grupos: pasado y futuro

S. González Jiménez[1]
I. González Vasco[2]
C. Martínez López[1]

[1] *Departamento de Matemáticas*
*Universidad de Oviedo*
*C/ Calvo Sotelo, s/n. 33007-Oviedo*
chelo@pinon.ccu.uniovi.es
[2] *Área de Matemática Aplicada*
*Universidad Rey Juan Carlos*
*C/ Tulipán s/n. 28933-Madrid*
migonzalez@escet.urjc.es

En los últimos años, especialmente ante la potencial aparición de los ordenadores cuánticos, nuevas herramientas algebraicas se han incorporado a la criptografía. Inicialmente, la Teoría de Números jugó el papel esencial y sigue siendo pieza clave en muchos de los criptosistemas mas ampliamente utilizados. Las nuevas amenazas a este tipo de esquemas ha estimulado la búsqueda de primitivas criptográficas en otras ramas de las Matemáticas (citemos, por ejemplo, los trabajos de P. Kocher sobre ataques 'por canales secundarios´ y de A. Shamir sobre hardware específico).

Paralelamente al avance de las técnicas de criptoanálisis se han desarrollado nuevas nociones de seguridad "demostrable"(*provable security*) con la finalidad de garantizar la fiabilidad de ciertos esquemas mediante demostraciones formales. Hoy en dia, la noción IND-CCA se ha convertido en la noción standard de seguridad. Una de las primeras propuestas de diseño para criptosistemas IND-CCA fue presentada por Cramer y Shoup, tomando como base grupos abelianos y prescindiendo en la demostración de idealizaciones (es decir, fuera del llamado *random oracle model*).

Nuestro objetivo es hacer una revisión de las distintas propuestas de criptosistemas basados en grupos, incluyendo una reciente metodología de diseño inspirada en la de Cramer y Shoup, utilizando grupos no necesariamente abelianos (propuesta de González-Vasco, Martínez, Steinwandt y Villar). Dicho marco constituye sin duda un paso mas hacia la construcción de criptosistemas seguros a partir de la teoría de grupos.