# HIMMO: A collusion-resistant identity-based scheme for symmetric key generation

Oscar García-Morchón
Ronald Rietman
Ludo Tolhuizen
*Philips Research*
*Eindhoven, The Netherlands*

Domingo Gómez
Jaime Gutiérrez
*University of Cantabria*
*Santander, Spain*

### Abstract

We describe HIMMO, a new scheme for identity-based symmetric key generation. Like the scheme of Blundo et al, HIMMO employs symmetric polynomials, which lead to very efficient implementations, but it is much less vulnerable against collusion attacks. HIMMO employs mixing modular operations over different rings and hiding part of the result of polynomial evaluation by only considering its least significant bits. We discuss the collusion resistance properties of HIMMO based on lattice-based cryptanalysis and provide figures on speed and memory usage of an implementation for various system parameters.

- C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. *"Perfectly-secure key distribution for dynamic conferences"*. In E.F. Brickell, editor, CRYPTO '92, volume 740 of Lecture Notes in Computer Science, pp. 471-486. Springer, 1992.
- O. García-Morchon, R. Rietman, L. Tolhuizen, D. Gómez Perez, J. Gutierrez, S. Merino del Pozo. *"An ultra-lightweight ID-based pairiwse key establishment scheme aiming at full collusion resistance"*. IACR Cryptology ePrint Archive, Vol 2012, p.618, 2012.