Year: 2011 | **Vol.: 79** | **Fasc.: 3-4**

Title: Post-quantum cryptography: lattice identification schemes

Author(s): Rosemberg Silva , Pierre-Louis Cayrel and Johannes Buchmann

This survey presents an overview and a comparative analysis of the state of art in post-quantum identification schemes based on lattices. Furthermore, we propose an adaptation of the HB family of identification in a lattice context. The aspects taken into account in such comparison are performance, security, communication costs, underlying hard-problem, completeness, soundness, and key sizes.

Address:
Rosemberg Silva
State University of Campinas (UNICAMP)
Institute of Computing
P.O. Box 6176
13084-971 Campinas
Brazil

Address:
Pierre-Louis Cayrel
Laboratoire Hubert Curien
UMR CNRS 5516
Bâtiment F 18 rue du professeur Benoît Lauras
42000 Saint-Etienne
France

Address:
Johannes Buchmann
CASED – Center for Advanced
Security Research Darmstadt
Mornewegstrasse, 32
64293 Darmstadt
Germany