“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Johannes A. Buchmann

(Technische Universitat Darmstadt)

“The Future of Digital Signatures.”

Apr 4, 12:00pm (New York Time).

Abstract:

Digital signatures are of great importance for the security of information technology and, in particular, the Internet. However, the digital signature schemes that are used in practice today are threatened by quantum computer attacks. Therefore, digital signature schemes are required that resist quantum computer attacks and can be used in practice. After explaining the relevance of digital signatures this talk discusses minimal security requirements for such schemes. The hash-based scheme XMSS is presented which has minimal security requirements. Experimental data show that XMSS is ready for being used in practice.

Next presentation: **Apr 18, 2013.** Ludovic Perret *(Université Pierre et Marie Curie)*
TBA

Algebraic Cryptography Center