Mathematics of Post-Quantum Cryptography

Algebraic Cryptography Center at Stevens Institute of Technology

---

Vladimir Shpilrain

(The City College of CUNY)

Cryptography using Chebyshev polynomials

Abstract:

Chebyshev polynomials T_m(x) and T_n(x) commute for any m and n. We use this fact to contemplate using Chebyshev polynomials in public-key cryptography.

Algebraic Cryptography Center

STEVENS Institute of Technology