1023-68-1853 **Bala Krishnamoorthy*** (bkrishna@math.wsu.edu), P.O. Box 643113, WSU, Pullman, WA 99164-3113, and **William Webb** and **Nathan Moyer**. *A Knapsack Cryptosystem Secure Against Attacks using Basis Reduction and Integer Programming.*

A knapsack cryptosystem encodes a message x (a 0–1 n-vector) as $M = a^T x$, where a are the knapsack coefficients (public). Its security depends on the fact that 0–1 knapsack problem is NP-complete. The coefficients of the Merkle-Hellman system are created from a set s of superincreasing weights ($s_i > \sum_{j<i} s_j$) disguised by a modular multiplication ($a_i = ps_i \bmod q$; p, q are private). Attacks were proposed on this cryptosystem using Diophantine approximation (Shamir), basis reduction (Lagarias and Odlyzko, and Coster et al.), and integer programming techniques; the superincreasing structure, and low density ($n/\log(\max_i a_i)$) being the weak points. We propose a knapsack cryptosystem without an underlying superincreasing sequence, and with additional cardinality constraints on x_j's. With $n = rm$,we want one x_j from each of r subsets (of size m) be equal to 1 (in addition to the knapsack equation). For appropriate parameters (r, m), the density of this knapsack is arbitrarily large. Attacks using basis reduction only find near-short vectors in the lattice with increasing probability (and not the shortest vector). Further, standard as well as basis reduction-based integer programming methods fail to solve these instances. (Received September 27, 2006)