Graph-Induced Multilinear Maps from Lattices

Shai Halevi, IBM Research

Graded multilinear encodings have found extensive applications in cryptography ranging from non-interactive key exchange protocols, to broadcast and attribute-based encryption, and even to software obfuscation. Despite seemingly unlimited applicability, essentially only two candidate constructions are known (GGH and CLT). In this work, we describe a new graph-induced multilinear encoding scheme from lattices. In a graph-induced multilinear encoding scheme the arithmetic operations that are allowed are restricted through an explicitly defined directed graph (somewhat similar to the "asymmetric variant" of previous schemes). Our construction encodes Learning With Errors (LWE) samples in short square matrices of higher dimensions. Addition and multiplication of the encodings corresponds naturally to addition and multiplication of the LWE secrets. Security of the new scheme is not known to follow from LWE hardness (or any other "nice" assumption), at present it requires making new hardness assumptions.

Joint work with Craig Gentry (IBM) and Sergey Gorbunov (MIT)