DAVID THOMSON, Carleton University

Low complexity normal bases over $\mathbb{F}_2$

This talk deals with basis representations of finite fields $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for computational purposes. We focus on *normal bases* that arise from the Galois orbit of a single field element. Explicitly, a normal basis is given by $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ for some $\alpha \in \mathbb{F}_{2^n}$. Normal bases are required when exponentiation, and in particular squaring, is a critical operation within an application. Examples where normal basis representation is prescribed include small characteristic Diffie-Hellman, elliptic curve computations and decoding random linear network codes.

Generic field multiplication can be expensive under normal basis representation. A measure of the cost of multiplication is the complexity (or density) of the multiplication tables of the basis. We will discuss an efficient algorithm to exhaustive search $\mathbb{F}_{2^n}$ for $n \leq 46$ (and counting...) for the minimum complexity normal basis.