Algebra and Number Theory Seminar

Title: Algebraic attacks against stream ciphers

Speaker: Pierre-Louis Cayrel (Université de Limoges)

Date: Mon 3rd March 2008 at 4:00PM

Location: Mathematical Sciences Seminar Room

Abstract: Algebraic attacks have been established as an important tool for cryptanalyzing LFSR-based keystream generators. All stream ciphers with linear feedback (one or several LFSR, linear cellular automata etc..) are concerned. Crucial for an efficient attack is to find appropriate equations of a degree as low as possible. Hereby, lower degrees are possible if many keystream bits are involved in one equation. It is known that valid equations correspond to annihilators of certain sets. The effort to compute the sets and to find annihilators on them are exponential in r (consecutive outputs), making efficient algorithms desirable.

Firs we present filtered and combined LFSRs and second we deal with algebraic attacks. Next, we describe several improvements for computing the equations of degree 3 for $r = 5, 6, 7$ in the case of the keystream generator E_0 employed in Bluetooth, where equations of degree 4 exist for $r = 4, 5$ and one equation of degree 3 for $rapprox 8, 822, 188$.

mailto: gary.mcguire at ucd.ie