Careers Evening

Richard Moloney

BSc and PhD Graduate
Software Engineer, Synopsys

My Career

- 2002 - 2006, BSc in Mathematics, UCD.
- 2006 - 2007, Travelling.
- 2007 - 2011, PhD in Number Theory and Cryptography, Claude Shannon Institute, UCD.
- 2008, Internship, Intel.
- 2011, R&D placement, RIM.
- 2012, Tutor at UCD Maths Support Centre, Volunteer at Aislinn Centre.
- 2012, R&D Software Engineer, Synopsys.

Why did I choose Mathematics?

- Because I enjoy doing mathematics!
- Because it's challenging.
- Because I think it is the best general purpose degree.

Some of the work I've done

- Cryptography using 'Edwards curves': Academic and applied work.
- Key exchange protocols.

  To communicate using a 'code', both people need to share some secret information. If Alice is in Australia and Bob is in Belgium, how do they arrange to share this secret?
- Kloosterman sums - demonstrated an unexpected connection with the trace function of finite fields.

What's a finite field?

Very roughly, a finite field is a finite set where you can add, subtract, multiply and divide elements, just as you can with real numbers. It's determined by an addition table and a multiplication table.

A field of size 3:

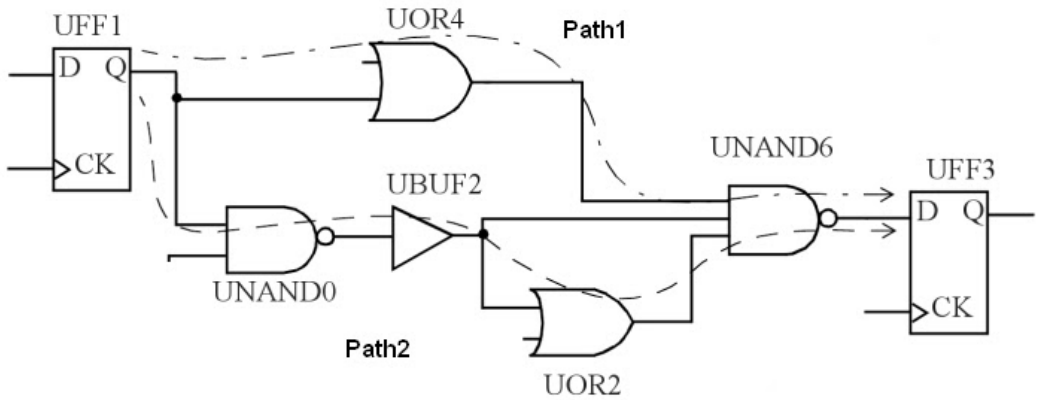
$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Question: Can you make a field of size 5? Of size 6?

What I'm doing now: Static Timing Analysis

Computer chips are a series of logic gates and memory elements ('registers') connected by wires. If two signals are to interact at a gate or register, they must arrive there within nanoseconds of each other.



This is an application of graph theory.