Nano-maths

Mathematics and nanotechnology are ideal partners, according to Dr Shaun Hendy of Victoria University and IRL. Anna Meyer explains.

What happens to physics when things get really small? How can we investigate structures so tiny that each individual atom is important? And how can useful nano-devices be built? Mathematics and computer simulation are helping to answer some of these fundamental nanotechnology questions.

"Using computer simulation, we can study materials right down at the nanoscale," Dr Shaun Hendy explains. "We might be interested in a nano-device containing millions of atoms; we can use the simulation to visualise how each of these atoms behaves." Part of the advantage of this 'silicon-laboratory' approach is the ability to see exactly what is going on at incredibly small scales, which is normally very difficult, expensive and time-consuming.

The computer simulations complement laboratory work by other research teams. "I work with several experimental groups in the MacDiarmid Institute for Advanced Materials and Nanotechnology, including Simon Brown's at the University of Canterbury."

"Simon's team builds nano-electronic devices using very small particles called nanoclusters. We're doing a lot of the modelling behind the manufacturing, to help figure out new and better ways of doing it. Some of the work we've done has led to new patents for his spin-off company."

Dr Hendy's team is one of the biggest computing consumers in New Zealand, using the University of Canterbury's Blue Gene supercomputer, the most powerful in the southern hemisphere. But even this is not always enough for the types of modelling the team is doing.

"We could use all the computing resources in the world and it would not be enough," said Dr Hendy, "so we're always trying to come up with clever ways of using the computer, of re-casting the mathematical problem in a slightly different way."

The team also constructs more traditional mathematical models of events at the nanoscale. In the world of the very small, even physics itself is different, and this can be used to make new types of devices. For example, surface tension becomes very important, as objects at that scale have very high surface area to volume ratios.

"We have had a lot of fun just constructing mathematical models of quite common phenomena, such as melting, and then seeing what happens when surface tension takes over," said Dr Hendy. "It's surprising how your intuition, which is tuned for a human-sized world, can get things completely wrong when you try to guess what will happen at the nanoscale."

Shaun Hendy, left, and Dmitri Schebarchov.

The group also work on what are known as homogenisation problems. "These are similar to what happens when you put batts between the wooden beams in your roof, creating a heterogeneous or mixed up layer of insulation in your ceiling. You may want to know how well this mixture of batts and beams insulates your roof on average."

"A similar situation occurs at the nanoscale, where atoms of different types are arranged in patterns. We are interested in how these patterns of atoms lead to the overall properties of a nanomaterial." NZIMA-funded postdoctoral fellow Dr Philip Zhang and PhD student Nat Lund have been active in this area.

Another focus is nanofluidic devices – tiny pipes already used for applications such as rapid DNA sequencing. As the pipes are made smaller, the pressure needed to push fluids through them increases dramatically. "People make these lovely little devices, but then the pump needed to run them is the size of a table – it's very embarrassing. Again, the problem is surface tension – the drag on the fluid increases as you make the channel smaller. We are trying to help reduce this problem."

Finally, NZIMA-funded PhD student Dmitri Schebarchov has been working on understanding the details of very small capillaries, such as carbon nanotubes. He and Dr Hendy have discovered a way to fill and unfill them with metals, which has not been achieved before. "This will be important for building different types of nanostructures," explained Dr Hendy, "and also has relevance to controlling nanotube growth, which can be difficult."

"There's a lot of fun to be had, and it is a good place for mathematical modellers as there are a lot of new mathematical problems to be found. The work is a mix of physics and mathematics – I like the challenge of solving mathematical problems for their own sake, but I also like the fact that there are applications at the end of it. It's also a field that is developing really rapidly. You certainly don't get bored - there's always something new that you can work on where you can make progress."

Secret keys and colluders

Anyone trying to keep track of their passwords for work, email, internet banking and other websites will understand the trade-off between security and efficiency. They have to remember more and more secret keys, which are secure unless one is forgotten, or they use the same key for every site, which is efficient but not secure. By Jenny Rankine.

Julia Novak is exploring the pure maths of Key Distribution Patterns - a method of reducing the amount of secret information that needs to be stored for secure communication between large networks of users. This could apply to any internet-based application, communication within large corporations, or in agencies where secret information needs to be protected such as the military.

While she is lecturing at the University of Auckland, and occasionally working for the NZIMA, her PhD in combinatorics is being supervised from Royal Holloway at the University of London. She is using incidence structures and block designs from design theory. Designs have points which can be associated with network users, while blocks are associated with security keys.

"There is always a trade off in secure communication networks between efficiency and security," Novak says. "Efficiency is a measure of how much secret information has to be produced, distributed and stored securely, and security can be measured by the minimum number of parties who share their secret keys - called colluders - that will break down the system's security.

All systems attempt to use as few unique keys as possible, while maximising the number of colluders needed to crack security. "A system is called x secure if x colluders will not be able to access anyone else's secure information."

Common systems use a mix of published and secret information. While keys remain secret, reference numbers for patterns of users to keys are published. "A one-way function is also published. It takes several keys as an input and outputs a digit key for each group of users who are trying to communicate securely."

Novak says the maths is "all about uniqueness and commonality". She specifies a group G, made up of families of privileged users, and a group F, made up of families of forbidden users, so that even if all members of F share information, they cannot access the keys of the privileged users.

None of the previous maths had taken into account the roles of individuals. For example, people who are less trustworthy may be put in group F, while people at the top of an organisation may not appear in any F family.

"This means setting upper and lower bounds. For example, what is the maximum number of keys users have to hold for a Group Key Distribution Pattern (GF-KDP) to work?" Usually the organisation contracting a secure system will specify at least one boundary.

These systems can be represented as binary matrices, with users as rows and keys as columns; a user with a key is represented by 1 and one without by 0. "For any binary matrix that meets certain conditions, I can read off a maximum set of privileged families. After I get that, I can find the maximum set of forbidden families for that set of privileged families. If the maximum set of forbidden families is specified first, then this restricts the maximum set of privileged families. From any one pattern of keys to users, you can have higher security and fewer secure communications, or more secure communications and lower security."

While the maths is still theoretical, it could be added to existing cryptographic security systems to improve their efficiency.

Awards and honours

BILL BARTON, director of the new NZIMA programme in Mathematics Education, has been elected the next President of the International Commission on Mathematical Instruction (ICMI), from 2010 to 2012.

NZIMA Co-Director **MARSTON CONDER** became the Royal Society of New Zealand's first Vice President International when his term as President of the RSNZ Academy ended on June 30 2008.

Professor **MIKE EASTWOOD**, one of the NZIMA 2008 Visiting Maclaurin Fellows, has won a Federation Fellowship from the Australian Research Council.

GAVEN MARTIN (one of the NZIMA principal investigators and co-director of the programme on Conformal Geometry) has been awarded the Hector Medal for 2008 in mathematical and information sciences, by the Royal Society of New Zealand.

NIC SMITH, director of one of the first NZIMA programmes (on modelling cellular function), has been invited to co-direct a programme on the Cardiac Physiome Project: Mathematical and Computational Foundations at the Isaac Newton Institute in Cambridge, UK from June to August 2009.