

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.

$$(a_{i,j}) = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$