Major step ahead for cryptography

May 26 2010

Imagine you could work out the answer to a question, without knowing what the question was. For example, suppose someone thinks of two numbers and then asks another person to work out their sum, without letting them know what the two numbers are. However, they are given an encryption of the two numbers but not told how to decrypt them.

Nigel Smart, Professor of Cryptology in the Department of Computer Science at the University of Bristol, will present a paper in Paris today, which makes a step towards a fully practical system to compute on encrypted data. The work could have wide ranging impact on areas as diverse as database access, electronic auctions and electronic voting.

Professor Smart said: "We will present a major improvement on a recent encryption scheme invented by IBM in 2009."

"Our scheme allows for computations to be performed on encrypted data , so it may eventually allow for the creation of systems in which you can store data remotely in a secure manner and still be able to access it."

This system could be used in medical care research. Hospitals or drug companies could perform statistical calculations on their shared databases without needing to reveal information about the individual patients. This would enable more efficient research in medical care and drug testing, without compromising patient privacy.

As another example, imagine a person is participating in an online auction but doesn't want the auctioneer to find out what their bid is in case it is used to encourage higher bids. Encrypted bids could be sent to the auctioneer and then, using a fully homomorphic scheme, the auctioneer could work out who won and what the winning bid was without learning what all the other bids were.

Alternatively in an electronic election all voters could encrypt their votes. The outcome of the election could then be computed by the returning officer whilst still ensuring the voter's privacy.

For nearly 30 years one cryptographic dream has been to come up with an encryption scheme for which you can "add" and "multiply" ciphertexts. Ciphertext is the encrypted result. This is a so-called fully homomorphic scheme. As soon as you can "add" and "multiply" you can compute any function.

Over the years many encryption schemes have been proposed which either have the "add" operation or the "multiply" operation, but not both. It was one of the Holy Grail's of cryptography to find a scheme where you could perform both operations.

In 2009 Craig Gentry from IBM came up with the first scheme which

simulataneously allows you to "add" and "multiply" ciphertexts. Gentry's scheme, although an amazing theoretical breakthrough is not practical.

In the paper to be presented, Professor Nigel Smart and Dr Frederik Vercauteren, from the Katholieke University Leuven in Belgium, have devised a way of simplifying Gentry's scheme so that it becomes more practical. Whilst the new scheme is not fully practical it is an important step along the way to forming a system which is truly practical.

Professor Smart and Dr Vercauteren's scheme also provides an intriguing new application of objects in an area of Pure Mathematics called Class Groups of Number Fields. Such objects have been studied in pure mathematics for around two century's with little possibility of impact on everyday life. This work is another example of the unexpected applicability of years of curiosity driven research.

The research is published at the 13th IACR workshop on Public Key Cryptography in Paris.

Provided by University of Bristol