Breakthrough in cryptography could result in more secure computing

September 9 2013

New research to be presented at the 18th European Symposium on Research in Computer Security (ESORICS 2013) this week could result in a sea change in how to secure computations.

The collaborative work between the University of Bristol and Aarhus University (Denmark) will be presented by Bristol PhD student Peter Scholl from the Department of Computer Science.

The paper, entitled 'Practical covertly secure MPC for dishonest majority – or: Breaking the SPDZ limits', builds upon earlier joint work between Bristol and Aarhus and fills in the missing pieces of the jigsaw from the groups prior work that was presented at the CRYPTO conference in Santa Barbara last year.

The SPDZ protocol (pronounced "Speedz") is a co-development between Bristol and Aarhus and provides the fastest protocol known to implement a theoretical idea called "Multi-Party Computation".

The idea behind Multi-Party Computation is that it should enable two or more people to compute any function of their choosing on their secret inputs, without revealing their inputs to either party. One example is an election, voters want their vote to be counted but they do not want their vote made public.

The protocol developed by the universities turns Multi-Party Computation from a theoretical tool into a practical reality. Using the

SPDZ protocol the team can now compute complex functions in a secure manner, enabling possible applications in the finance, drugs and chemical industries where computation often needs to be performed on secret data.

Nigel Smart, Professor of Cryptology in the University of Bristol's Department of Computer Science and leader on the project, said: "We have demonstrated our protocol to various groups and organisations across the world, and everyone is impressed by how fast we can actually perform secure computations.

"Only a few years ago such a theoretical idea becoming reality was considered Alice in Wonderland style over ambitious hope. However, we in Bristol realised around five years ago that a number of advances in different areas would enable the pipe dream to be achieved. It is great that we have been able to demonstrate our foresight was correct."

The University of Bristol is now starting to consider commercialising the protocol via a company Dyadic Security Limited, co-founded by Professor Smart and Professor Yehuda Lindell from Bar-Ilan University in Israel.

More information: Practical Covertly Secure MPC for Dishonest Majority – or: Breaking the SPDZ Limits, Ivan Damgard, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart, ESORICS 2013, 9-13 September 2013. A copy of the paper can be downloaded from the following URL: fluff.bris.ac.uk/fluff/u3/injf … pJj2KGMP6QmfB1MQHUR/

Provided by University of Bristol