CFEM workshop: Theory and Practice of Multiparty Computation
4 to 8 June, 2012
Aarhus University, Denmark

Speaker: Dan Bogdanov, Cybernetica

Title: Easily programmable secure multi-party computation on integers, strings and floating point numbers

Secure computation techniques have been shown to be practical in several applications. The next step towards wide-scale adoption of the technology is the creation of developer tools that can be used in the creation of information systems. We present the Sharemind framework and the SecreC programming language as tools for programming secure computation.

The framework is built to be flexible with regard to the underlying cryptographic technique. While the default implementation uses general secure multi-party computation, other methods can easily be integrated with the runtime and the programming languages. A unique feature of Sharemind is the possibility to easily combine different secure computation techniques in a single application. Sharemind can perform private operations on truth values, integers of various sizes, floating point numbers and strings. These operations are available in the programming language.

Sharemind and its tools have been validated in a successful real-life deployment in 2011 when a secure financial information aggregation system was built and deployed for the Estonian Association of ICT companies.