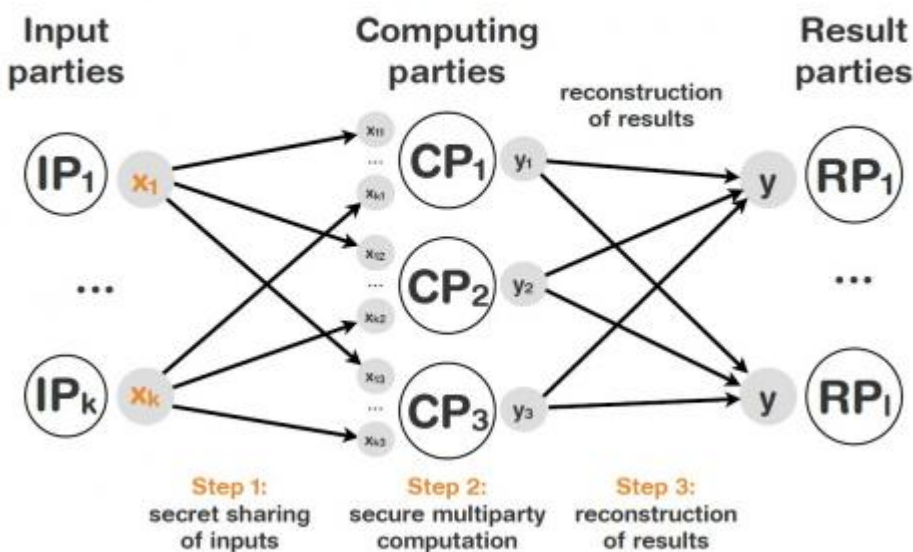


## Baltic countries in focus: UaESMC FET Open project

Each of us has some information it considers private and is willing to share only reluctantly, be it about one's health, or personal preferences, or commercial interests or capabilities. Our society has put in place rules on how such data can be transmitted or processed. While these rules protect the privacy of data, at times, they seriously diminish the benefits that can be obtained from studying it. Can the existing balance between privacy and usability be improved?

### the sharemind model



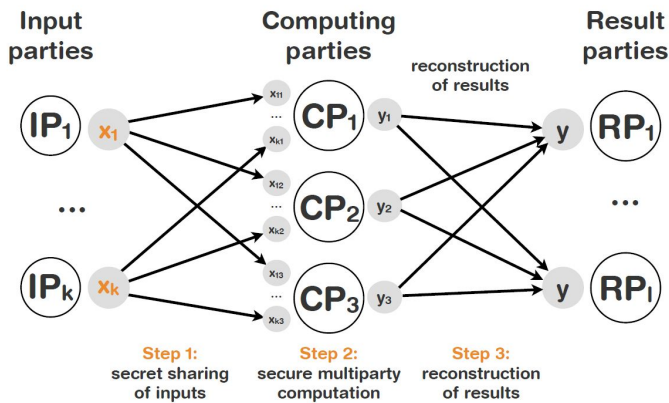
Doctor Peeter Laud, the coordinator of UaESMC project, is the Research Director of Cybernetica. His main research direction has been the cryptographically correct analysis of programs and protocols containing cryptographic primitives. In this article, Dr. Laud explains in detail the objectives and outcomes of UaESMC project.

*"As a theoretical construction, the possibility to perform any multi-party computation without learning anything about other parties' inputs has been known for long time, with the security being based on cryptographic assumptions and/or the honesty of some unknown set of parties. A lot of work has gone into minimizing and better understanding these assumptions. Relatively less effort has been put into bringing the performance of secure multiparty computation (SMC) to a level where it could be used to solve problems of various kinds and realistic sizes."*

*"The Usable and Efficient Secure Multiparty Computation (UaESMC) project has aimed to bring the techniques and tools for SMC to a level where they can be applied to decisional and computational problems of practical size in several different social and economic sectors. Now in its third year, the project has taken secure protocols for primitive computational steps provided by theoretical constructions of SMC, and shown how to combine them in order to perform in privacy-preserving manner tasks as varied as statistics and data mining, regular language processing, analysis of business processes, graph algorithms, network management, etc. Working with privacy-preserving tools may be quite different compared to having all data available for analysis. The UaESMC project has devised privacy-preserving analogues for data visualization tools aimed in particular towards*

statistical analysts."

### the sharemind model



Protocols developed in UaESMC follow the Sharemind model for SMC: a dedicated set of computing parties receive the shares of inputs and execute protocols to produce shares of outputs. Parties interested in the result receive the output shares. This model allows easy composition of large privacy-preserving applications from protocols for specific tasks.

"The UaESMC project has been funded under the FET Open High-Tech SME scheme, and is running for 42 months. It is executed by a consortium of four partners from three different countries (Estonia, Sweden and Greece), coordinated by Cybernetica, an Estonian SME. Both the organizational and the geographical qualities have been particularly helpful in picking the direction of the project and achieving its results. The SME environment has made us to consider the practical applicability of our results. In particular, Cybernetica has provided the project with the existing SMC platform Sharemind, that we have used to experiment with our protocols. Estonia has provided us with a society that is aware of security implications of information technologies and willing to try out novel methods for ensuring the privacy of its constituents."

"The technologies developed in UaESMC will be used already in 2015 to learn about the trends in society without breaching the privacy of individuals. By combining the data on academic success of current and past ICT students with the amount of taxes they've paid through different employers, we hope to learn where the ICT students find employment, how early they are being employed, and if this affects their study success and future earning potential."

### Try the UaESMC tool demo!

This application showcases the privacy-preserving analysis of confidential information using secure computation technology. The tool shows how information can be securely collected from multiple sources and analyzed so that nobody except for the data owner can see the individual values. Cryptographic secure computation ensures that even the servers hosting the data do not have to see it in order to compute statistical analysis results. See the video below for an explanation.

The UaESMC project has devised efficient privacy-preserving protocols for a wide variety of computational tasks of realistic size.

## Metadata

## **Related topics**

FET Open

Future and Emerging Technologies

---

### **Source URL:**

*<https://digital-strategy.ec.europa.eu/news/baltic-countries-focus-uaesmc-fet-open-project>*